NETGEAR®

N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B

User Manual

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the Support website at
http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): Check the list of phone numbers at
http://support.netgear.com/app/answers/detail/a_id/984.

Trademarks

Statement of Conditions

Contents

Chapter 4 Content Filtering

Chapter 5 Network Maintenance

Chapter 6 USB Storage

Chapter 7   Advanced Settings

Chapter 8   Virtual Private Networking

Chapter 9 Troubleshooting

Appendix A Supplemental Information

Appendix B VPN Configuration

Appendix C Notification of Compliance

Hardware Setup

Getting to know your modem router

<div style="text-align: right; font-size: large;">1</div>

The NETGEAR N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B offers dual-band technology and ensures top speeds and the greatest range for demanding applications, such as streaming HD video and multiplayer gaming. Complete with a built-in ADSL modem, it is compatible with all major ADSL Internet service providers. The gigabit port on the WAN side has an option to connect to a fiber/cable modem.

NETGEAR green features:

- Power On/Off button
- 80% recycled packaging
- CEC (California Efficiency)
- RoHS
- WEEE

If you have not already set up your new router using the installation guide that comes in the box, this chapter walks you through the hardware setup. *Chapter 2, Router Internet Setup,* explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your New Router*
- *Hardware Features*
- *Position Your Modem Router*
- *ADSL Microfilters*
- *Cable Your Modem Router*
- *Verify the Cabling*

For more information about the topics covered in this manual, visit the support website at *http://support.netgear.com*.

Unpack Your New Router

Your box should contain the following items:

- N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Telephone cable with RJ-11 connector
- Installation guide with cabling and router setup instructions

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair. See *Position Your Modem Router* on page 12 for information about where to place and how to position your router.

Modem Router

AC Power adapter

Ethernet cable

Telephone cable
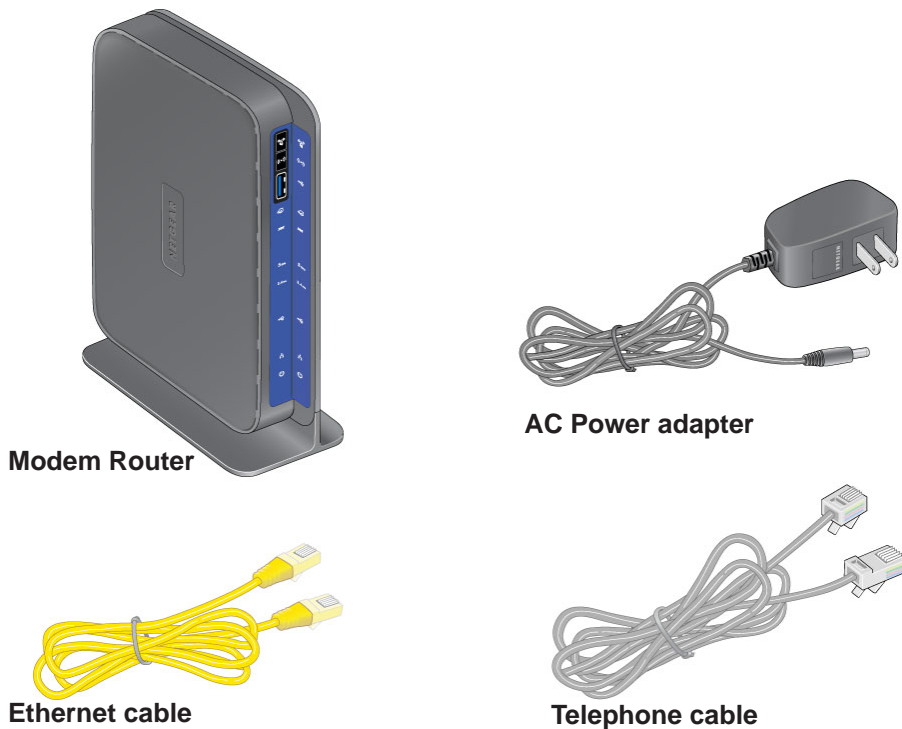
Figure 1. Box contents

Hardware Features

Before you cable your router, take a moment to become familiar with the label and the front and back panels. Pay particular attention to the LEDs on the front panel.

Front Panel

The modem router front panel has the 10 status LEDs, icons, and ports shown in the figure. Note that the Wireless and WPS icons are buttons.

WPS On/Off button

Wireless On/Off button

USB port

Internet
DSL

5 GHZ wireless
2.4 GHz wireless

USB

LAN ports
Power
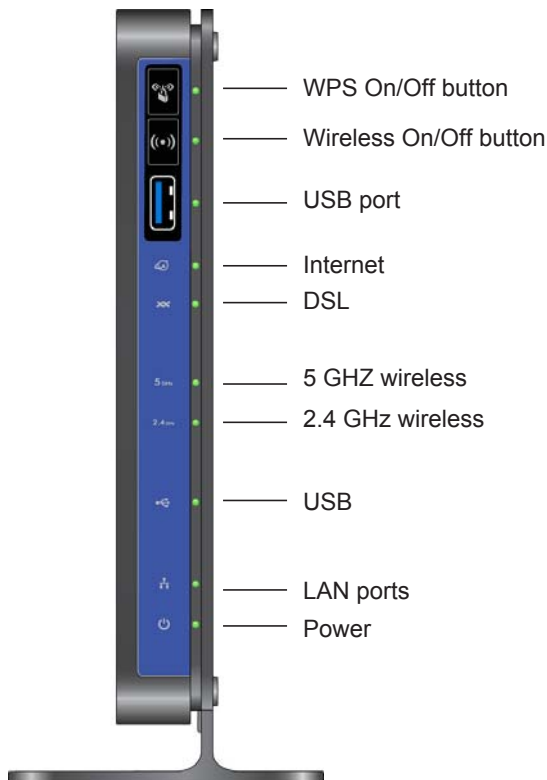
Figure 2. Front panel

Front Panel Buttons and USB Port

WPS button. You can use this button to add a wireless computer or device to your network using Wi-Fi Protected Setup. The wireless computer or device has to support WPS. see *Wi-Fi Protected Setup (WPS) Method* on page 33..
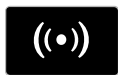
Wireless On/Off button. This button turns the wireless radio of the modem router off and on. See *Turn Off Wireless Connectivity* on page 31
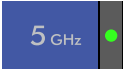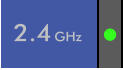
USB port. You can use this port to connect USB storage devices like flash drives or hard drives.

Front Panel LEDs

The following table describe the LEDs on the front panel from top to bottom.

Table 1. LED Descriptions

LED	Description
Internet	• **Solid green**. You have an Internet connection. If this connection is dropped due to an idle time-out but the connection is still present, the light stays green. If the Internet connection is dropped for any other reason, the light turns off. • **Solid red**.The Internet (IP) connection failed. See *No ISP Connection* on page 139 for troubleshooting information. • **Blinking green**. Data is being transmitted over the Internet connection. • **Off**. No Internet connection is detected or the device is in bridge mode (an external device handles the ISP connection)
DSL	• **Solid green**. You have an ADSL connection. In technical terms, the ADSL port is synchronized with an ISP's network-access device • **Blinking green**. Indicates that the modem router is negotiating the best possible speed on the ADSL line. • **Off**. The unit is off or there is no IP connection.
5 GHz Wireless	• **Solid blue**. There is wireless connectivity. • **Blinking blue**. Data is being sent or received over the 5 GHz wireless link. • **Off**. There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity.
2.54 GHz Wireless	• **Solid green**. There is wireless connectivity. • **Blinking green**. Data is being sent or received over the 2.4 GHz wireless link. • **Off**. There is no wireless connectivity. You can still plug an Ethernet cable into one of the LAN ports to get wired connectivity.
USB	• **Solid green**. A USB port has detected a USB device. • **Blinking green**. Data is being transmitted or received. • **Off**. No link is detected on these ports.
LAN (Ethernet)	• **Solid green**. A LAN port has detected an Ethernet link with a device. • **Blinking green**. Data is being transmitted or received. • **Off**. No link is detected on these ports.
Power	• Solid green. Power is supplied to the modem router. • Solid red. POST (power-on self-test) failure or a device malfunction has occurred • Off. Power is not supplied to the modem router. • Restore Factory Settings. The Power LED blinks momentarily when the Restore Factory Settings button on the bottom of the unit is pressed for 6 seconds. The Power LED blinks red three times when the Restore Factory Settings button is released and then turns green as the modem router resets to its factory defaults.

Back Panel

The back panel has the Power On/Off button and port connections shown in the figure:

1. ADSL line

2. Gigabit port for connecting to external cable/fiber modem

3. Gigabit Ethernet ports

4. USB port

5. Power On/Off button
6. AC power adapter input
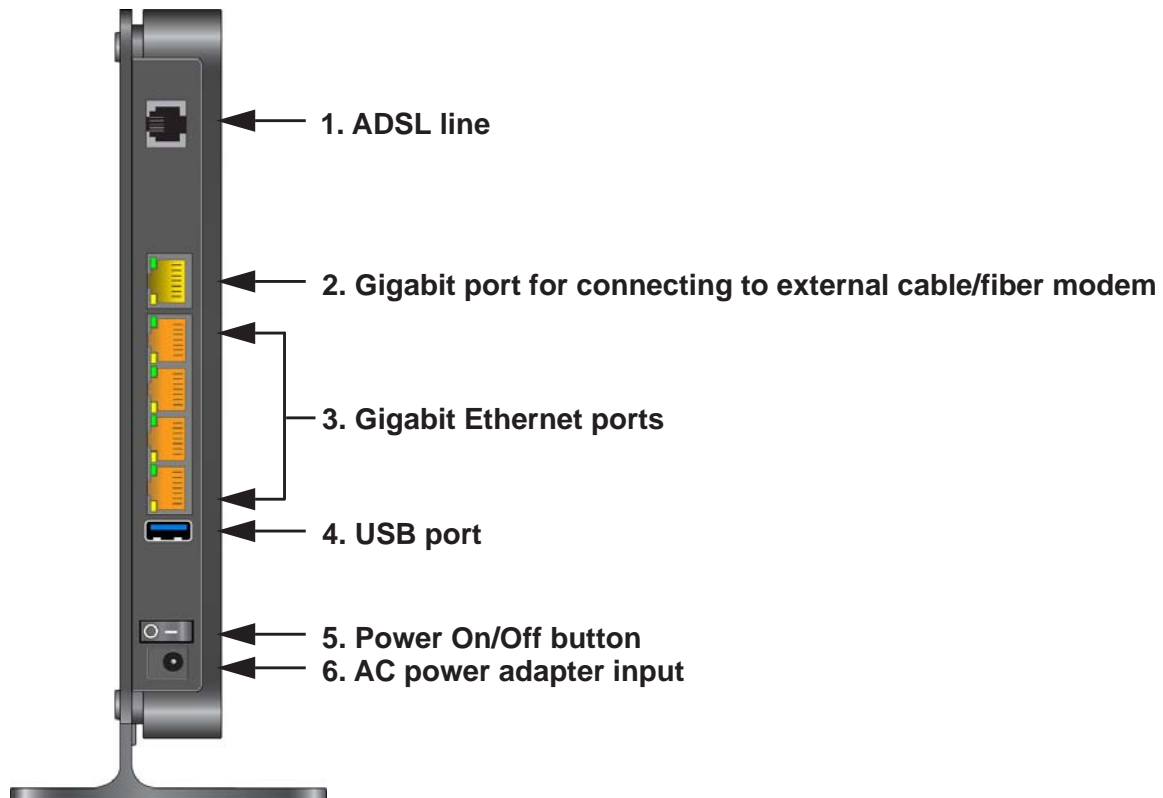
Figure 3. Back panel port connections

Viewed from left to right, the rear panel contains the following elements:

1. RJ-11 asynchronous DSL (ADSL) port for connecting the modem router to an ADSL line

   Note: An ADSL port is capable of sending data over an ADSL line at one speed and receiving it at another speed.

2. Ethernet WAN port for connecting the modem router to a fiber/cable modem

   Note: You can use either the ADSL or Gigabit Ethernet port for WAN connectivity.

3. Four Ethernet RJ-45 LAN ports for cabling the modem router to the local computers
4. USB port for connecting USB storage devices like flash drives or hard drives
5. Power On/Off button
6. AC power adapter input

Label

The label on the bottom of the modem router shows the router's Restore Factory Settings button, WPS security PIN, MAC address, and serial number.
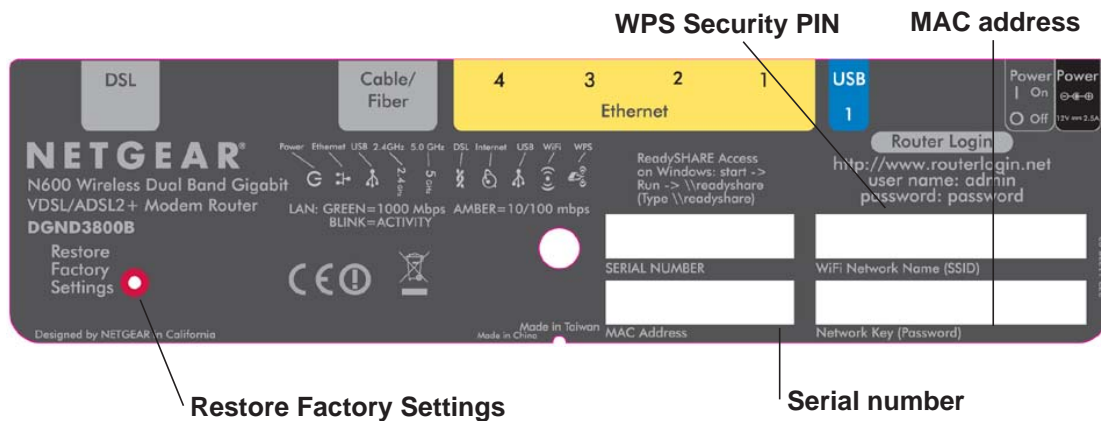
Figure 4. Label on modem router bottom

See *Factory Settings* on page 147 for information about the Restore Factory Settings button and the factory setting values.

Position Your Modem Router

You should operate the modem router only in a vertical position, resting on its stand.

The modem router lets you access your wireless network within its range. The range can vary depending on the location of your modem router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your modem router:

• Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.

• So it is accessible to an AC power outlet and near Ethernet cables for wired computers.

• In an elevated location such as a high shelf, keeping the number of walls and ceilings between the modem router and your other devices to a minimum.

• Away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwave ovens, computers, or the base of a cordless phone or 2.4 GHz cordless phone.

• Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

If you use multiple access points, set up adjacent access points with different radio frequency channels to reduce interference. NETGEAR recommends five channels of spacing for adjacent access points (for example, use Channels 1 and 6, or 6 and 11).

ADSL Microfilters

If this is the first time you cable a modem router between an ADSL phone line and your computer, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your Modem Router* on page 14.

An ADSL microfilter is a small in-line device that filters ADSL interference out of standard phone equipment that shares the same line with your ADSL service. Every telephone device that connects to a telephone line that provides ADSL service needs an ADSL microfilter to filter out the ADSL interference. Example devices are telephones, fax machines, answering machines, and caller ID displays. Note that not every phone line in your home necessarily carries ADSL service. That depends on the ADSL service setup in your home.

For many products, the ADSL microfilter is included in the box with the modem router. If you purchased the modem router in a country where a microfilter is not included, you have to acquire the ADSL microfilter separately.

One-Line ADSL Microfilter (Not Included)

Plug the ADSL microfilter into the wall outlet and plug your phone equipment into the jack labeled Phone. The modem router plugs directly into a separate ADSL line. Plugging the modem router into the phone jack blocks the Internet connection. If you do not have a separate ADSL line for the router, the best thing to do is to use an ADSL microfilter with a built-in splitter.

Plugs into the ADSL line

Figure 5. One-line ADSL microfilter

Second best when you do not have a separate ADSL line for the router is to get a separate splitter. To use a one-line filter with a separate splitter, insert the splitter into the phone outlet, connect the one-line filter to the splitter, and connect the phone to the filter.

Two-Line ADSL Microfilter (Included)

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the modem router and your telephone equipment. Plug the ADSL microfilter into the wall outlet, plug your phone equipment into the jack labeled Phone, and plug the modem router into the jack labeled ADSL.

Plugs into the ADSL line

Figure 6. Two-line ADSL microfilter with built-in splitter

Summary

- One-line ADSL microfilter (not included). Use with a phone or fax machine.
- Splitter (not included). Use with a one-line ADSL microfilter to share an outlet with a phone and the modem router.
- Two-line ADSL microfilter with built-in splitter (included). Use to share an outlet with a phone and the modem router.

Cable Your Modem Router

WARNING!

DO *not* stack equipment, or place equipment in tight spaces, or in drawers. Be sure your equipment is surrounded by at least 2 inches of air space. The unit should not be wall mounted.

The installation guide that came in the box includes a cabling diagram similar to the following figure:
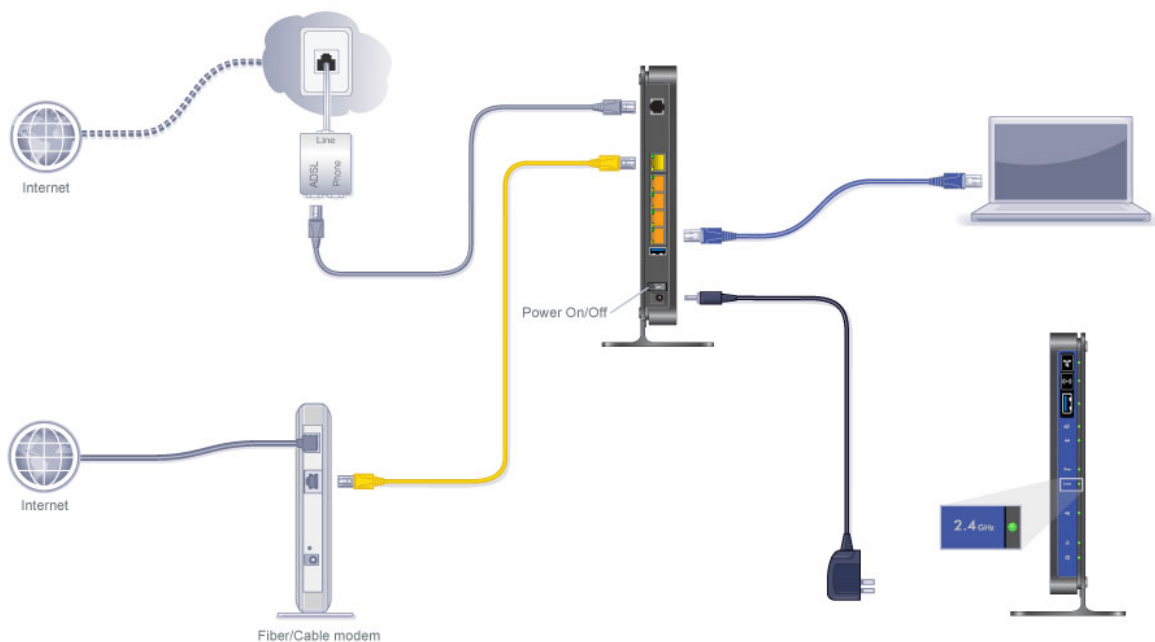
Figure 7. Cabling diagram

CAUTION:

Incorrectly connecting a filter to your modem router blocks your ADSL connection.

Verify the Cabling

Verify that your router is cabled correctly by checking the modem router LEDs. Turn on the modem router by pressing the **Power On/Off** button on the back.

- The Power LED is green when the modem router is turned on.
- The LAN port is green when a computer is cabled to the router by an Ethernet cable.
- The Wireless LEDs are lit when the modem router is turned on.
- The DSL LED is green when you have an ADSL connection.
- The Internet LED is red when there is no Internet connection.

Turn on your computer. If software usually logs you in to your Internet connection, do not run that software. Cancel it if it starts automatically.

Router Internet Setup

Connecting to the network

<div style="text-align:right"># 2</div>

This chapter explains how to set up your Internet connection using one of two methods: Setup Wizard or manual setup. If you have already set up your router using one of these methods, the initial router setup is complete. Refer to this chapter if you want to become familiar with the router menus, view or adjust the initial settings, or change the router password and login time-out.

This chapter contains the following sections:

- *Router Setup Preparation*
- *Log In to the N600 Modem Router*
- *Upgrade Router Firmware*
- *Router Interface*
- *Setup Wizard*
- *Manual Setup (Basic Settings)*
- *ADSL Settings*
- *Unsuccessful Internet Connection*
- *Change Password and Login Time-Out*
- *Log Out Manually*
- *Types of Logins*

Router Setup Preparation

You can set up your modem router with the Setup Wizard as described in *Setup Wizard* on page 21 or manually as described in *Manual Setup (Basic Settings)* on page 22. However, before you start the setup process, you need to have your ISP information on hand and make sure the computers, and other devices in the network have the settings described here.

> **Note:** If you have a Macintosh or Linux system, you have to use the manual setup method.

Use Standard TCP/IP Properties for DHCP

If you configured your computer to use a static IP address, you need to change the settings back so that it uses Dynamic Host Configuration Protocol (DHCP). See *Appendix A, Supplemental Information* for more information.

Replace an Existing Router

To replace an existing router, disconnect it completely from your network and set it aside before starting the router setup.

Adapters and Security Settings

A wireless adapter is the wireless radio in your computer that lets the computer connect to a wireless network. Most computers come with an adapter already installed, but if it is outdated or slow, you can purchase a USB adapter to plug into a USB port.

Make sure the wireless adapter in each computer in your wireless network supports the same security settings as the modem router.

> **Note:** If you connect devices to your modem router using WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 33, those devices assume the security settings of the router.

Gather ISP Information

You need the following information to set up your modem router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information needed to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no

longer need to launch the ISP's login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in.

- Active Internet service provided by an ADSL account
- The ISP configuration information for your ADSL account
    - ISP login name and password
    - ISP Domain Name Server (DNS) addresses
    - Fixed or static IP address
    - Host and domain names
    - Depending on how your ISP set up your Internet account, you could need to know one or more of these settings for a manual setup:
        - Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters
        - Multiplexing method
        - Host and domain names

Log In to the N600 Modem Router

Log in to the modem router to view or change settings or to set up the modem router.

➢ **To log in:**

1. Type **http://192.168.0.1** in the address field of your browser and press **Enter** to display the login window. You can also enter either of these addresses to access the modem router: **http://www.routerlogin.net** or **http://www.routerlogin.com**.
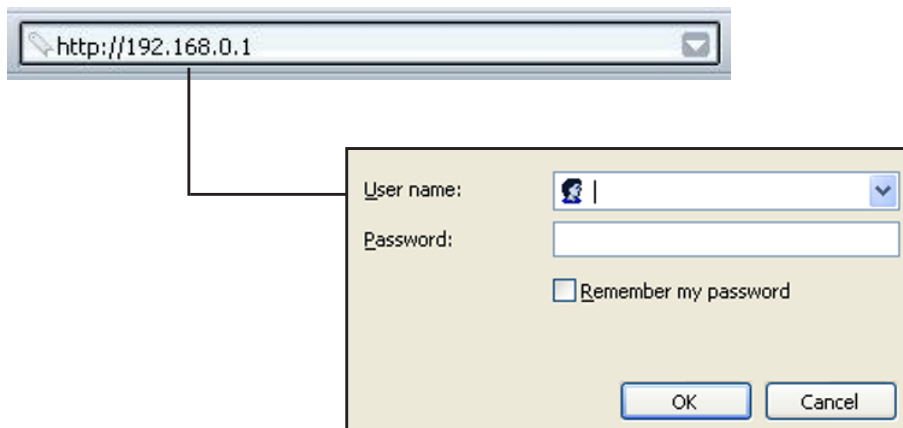
2. When prompted, enter **admin** for the router user name and **password** for the router password, both in lowercase letters, and click **OK**.

Note: The router user name and password are probably different from the user name and password for logging in to your Internet connection. See *Types of Logins* on page 28 for more information.

The router screens display, where you can do things like changing settings or adding other devices to your network. For a brief description of the available functionality, see *Router Interface* on page 20. For information about adding devices to your network, see *Wi-Fi Protected Setup (WPS) Method* on page 33.

If you do not see the login prompt:

1. Check the LEDs on the router front panel to make sure that the modem router is plugged into an electrical outlet, its power is on, and the Ethernet cable between your computer and the router is connected to a LAN port.

2. If you connected the Ethernet cable and quickly launched your browser and typed in the router URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.

3. If you are having trouble accessing the router wirelessly, NETGEAR recommends that during setup you use an Ethernet cable to connect your computer so that you can log in to the modem router.

Note: If you cannot connect to the modem router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your computer Control Panel. They should be set to obtain both IP and DNS server addresses automatically.

Upgrade Router Firmware

When you log in and if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest available firmware. For more information about upgrading firmware, see *Chapter 5, Network Maintenance*.

➢ **To upgrade the firmware:**

1. Click **Yes** to check for new firmware (recommended). The modem router checks the NETGEAR database for new firmware.

2. If no new firmware is available, click **No** to exit. You can check for new firmware later.

3. If new firmware is available, click **Yes** to upgrade the router with the latest firmware. After the upgrade, the router restarts.

⚠️ **CAUTION:**

Do not try to go online, turn off the router, shut down the computer, or do anything else to the router until the router finishes restarting.

You cannot upgrade firmware until you have established your Internet connection as described in *Setup Wizard* on page 21.

Router Interface

The router interface gives you access to the router's current settings so you can view or change them (if needed). The left column has the router menus, and the right column provides online help. The middle column is the screen for the current menu option.
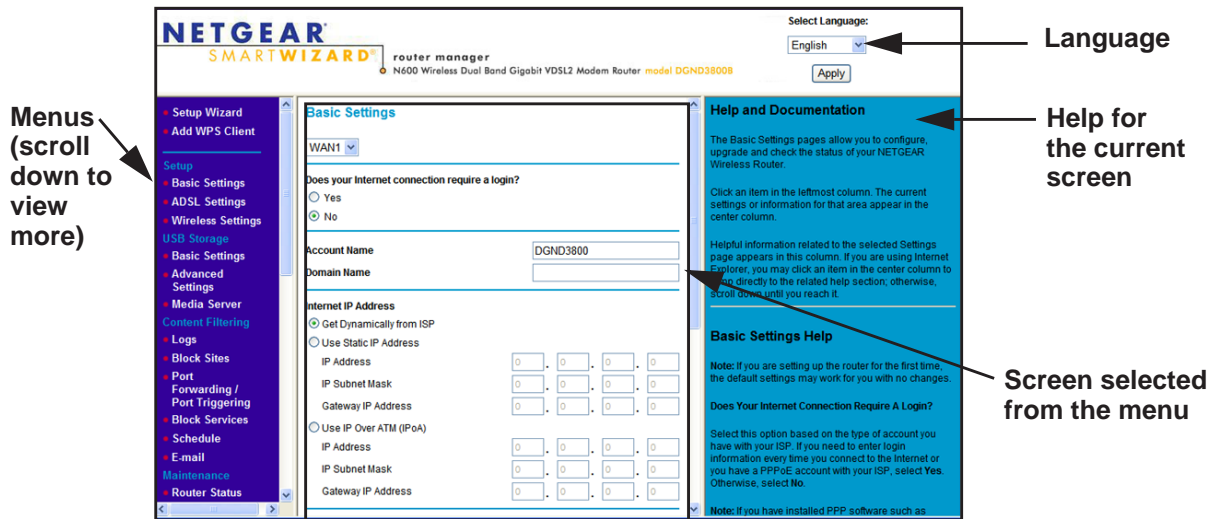
Figure 8. Router interface

Setup Wizard

Specify the language and location, and automatically detect the Internet connection. See *Setup Wizard* on page 21.

Add WPS Client

Add WPS-compatible wireless devices and other equipment to your wireless network. See *Add Clients (Devices) to Your Network* on page 33.

Setup Menu

Set, upgrade, and check the ISP and wireless network settings of your router. See *Manual Setup (Basic Settings)* on page 22 and *ADSL Settings* on page 25. See also *Chapter 3, Wireless Settings*.

USB Storage Menu

Add removable storage to your network. See *Chapter 6, USB Storage*.

Content Filtering Menu

View and configure the router firewall settings to prevent objectionable content from reaching your computers. See *Chapter 4, Content Filtering*.

Maintenance Menu

Administer and maintain your router and network. See *Chapter 5, Network Maintenance*.

Advanced Menu

Set the router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. See *Chapter 7, Advanced Settings*. Using this menu requires a solid understanding of networking concepts.

Advanced – VPN Menu

Set up secure encrypted communications. See *Chapter 8, Virtual Private Networking*. Using this menu requires a solid understanding of networking concepts.

Web Support

Go to the NETGEAR support site to get information, help, and product documentation. These links work once you have an Internet connection.

Setup Wizard

You have to log in to the modem router to set the country, language, and Internet connection.

➢ **To use the Setup Wizard:**

1. Select **Setup Wizard** from the top of the router menus to display the following screen:

2. Select your country and language:
   - **Country**. It is important to specify the location where the modem router operates so that the Internet connection works correctly. The default is Germany.
   - **Language**. The default is English. You can select another language if you prefer.
3. Select either **Yes** or **No, I want to configure the Router myself**. If you select No, proceed to *Manual Setup (Basic Settings)* on page 22.
4. If you selected Yes, click **Next**.

You are prompted to change the administrator password:

Change the Administrator Password

Your NETGEAR router uses an administrator password. It is printed on the bottom
label of the router. The default password is "password". The password is case
sensitive. For example, **PASSWORD** is not the same as **passWORD**.

You can change the password to restrict access to the configuration options
of the router.

Enter a new password or click Next to keep the default password

Password:
Repeat New Password:

[Back]   [Next]

5. Enter the current password, and then enter the new password and click **Next**.

    With automatic Internet detection, the Setup Wizard searches your Internet connection
    for servers and protocols to determine your ISP configuration.

    Note: The Setup Wizard cannot detect a Point-to-Point Tunneling Protocol
    (PPTP) connection. If your ISP uses PPTP, you have to set your
    Internet connection through the screen described in *Manual Setup
    (Basic Settings)* on page 22.

Manual Setup (Basic Settings)

The Basic Settings screen displays when you select No. I want to configure the Router myself
in the Setup Wizard and is also available from the router menus. It is where you view or
change ISP information. The fields that display vary depending on whether or not your
Internet connection requires a login.

Note: Check that the country and language are set as described *Setup
Wizard* on page 21 before proceeding with the manual setup.

➢ **To set up the basic settings manually:**

1. Select **Set Up > Basic Settings** and select **Yes** or **No** depending on whether or not
    your ISP requires a login.
    *   **Yes**. Select the encapsulation method and enter the login name. If you want to
        change the login time-out, enter a new value in minutes.
    *   **No**. Enter the account and domain names, as needed.

The available fields change based on whether you selected Yes or No for a login.

ISP *does not* require login   **ISP *does* require login**

2. Enter the settings for the IP address and DNS server. The default ADSL settings usually work fine. If you have problems with your connection, check the ADSL settings and see *ADSL Settings* on page 25 for more information.

3. If no login is required, you can specify the MAC Address setting.

4. Click **Apply** to save your settings.

5. Click **Test** to test your Internet connection. If the NETGEAR website does not appear within 1 minute, and see *Troubleshooting* on page 136.

Basic Setting Screen Fields

The following descriptions explain all of the possible fields in the Basic Settings screen. Note that which fields appear in this screen depends on whether or not an ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

• *When no login is required, these fields display:*

Account Name (If required). Enter the account name provided by your ISP. This might also be called the host name.

Domain Name (If required). Enter the domain name provided by your ISP.

* *When your ISP requires a login, these fields display*:

    Encapsulation. Encapsulation is a method for enclosing multiple protocols. PPP stands for Point-to-Point Protocol. The choices are PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM).

    Login. The login name provided by your ISP. This is often an email address.

    Password. The password that you use to log in to your ISP.

    Connection Mode. Specify whether your Internet connection is always on, or is off by default unless you are using it.

    Idle Timeout (In minutes). If you want to change the login timeout, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Note: The German version of this product includes an Automatic Internet connection reset setting. This can be used to set the specific time that the modem router automatically disconnects from the Internet.

Internet IP Address.

* *When a login is required, these fields display*:

    Get Dynamically from ISP. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.

    Use Static IP Address. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's modem router to which your modem router will connect.

* *When a login is not required, this field displays*:

    Use IP Over ATM (IPoA). Your ISP uses classical IP addresses (RFC 1577). Enter the IP address, IP subnet mask, and gateway IP addresses that your ISP assigned.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

* **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.

* **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

NAT (Network Address Translation). NAT automatically assigns private IP addresses (10.1.1.x) to LAN-connected devices.

*   **Enable**. Usually NAT is enabled.
*   **Disable**. This disables NAT, but leaves the firewall active. Disable NAT only if you are sure you do not need it. When NAT is disabled, only standard routing is performed by this modem. Classical routing lets you directly manage the IP addresses that the modem router uses. Classical routing should be selected only by experienced users.[1]
*   **Disable firewall**. This disables the firewall in addition to disabling NAT. With the firewall disabled, the protections usually provided to your network are disabled.

When no login is required, this field displays:

Router MAC Address. The Ethernet MAC address used by the modem router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They then accept traffic only from the MAC address of that computer. This feature allows your modem router to use your computer's MAC address (this is also called cloning).

*   **Use Default Address**. Use the default MAC address.
*   **Use Computer MAC Address**. The modem router captures and use the MAC address of the computer that you are now using. You have to be using the one computer that is allowed by the ISP.
*   **Use This MAC Address**. Enter the MAC address that you want to use..

ADSL Settings

The ADSL settings of your modem router work fine for most ISPs. However, some ISPs use a specific multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI).

Note: You need to use the Setup Wizard to select the correct country for the default ADSL settings to work.

---

1. Disabling NAT reboots the modem router and resets its configuration settings to the factory defaults. Disable NAT only if you plan to set up the modem router in a setting where you will be manually administering the IP address space on the LAN side of the modem.

➢ **To enter a multiplexing method or VPI/VCI number (if provided by the ISP):**

1. Select **Setup > ADSL Settings** to display the following screen:

2. In the Internet Service Provider drop-down list, select your ISP.
3. Specify the transfer mode.

   The transfer mode can be PTM (Packet Transfer Mode) or ATM (Asynchronous Transfer Mode). The VDSL2 interface supports PTM. PTM transports packets (IP, PPP, Ethernet, MPLS, and so on) over DSL links as an alternative to using ATM. PTM is based on the Ethernet in the First Mile (EFM) IEEE802.3ah standard.

4. Select the DSL mode. The available settings depend on the selection in the Transfer Mode field.
   - If the Transfer Mode is ATM, the DSL mode can be Auto, ADSL, ADSL2, or ADSL2+.
   - If the transfer mode is PTM, the DSL mode is VDSL (Very-high-bit-rate digital subscriber line).

5. In the Multiplexing Method drop-down list, select **LLC-based** or **VC-based**.
6. For the VPI, type a number between 0 and 255. The default is 8 for the U.S. version, 0 for the worldwide version, and 1 for the German version.
7. For the VCI, type a number between 32 and 65535. The default is 35 for the U.S. version, 38 for the worldwide version, and 32 for the German version.
8. Click **Apply**.

Unsuccessful Internet Connection

1. Review your settings to be sure you have selected the correct options and typed everything correctly.

2. Contact your ISP to verify that you have the correct configuration information.

3. Read *Chapter 9, Troubleshooting*. If problems persist, register your product and contact NETGEAR technical support.

Note: If you cannot connect to the modem router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your Windows Control Panel. They should be set to obtain *both* IP and DNS server addresses automatically.

Change Password and Login Time-Out

For security reasons, the modem router has its own user name and password that default to **admin** and **password**. You can and should change this password to a secure password that is easy to remember. The ideal password contains no dictionary words from any language and is a mixture of uppercase and lowercase letters, numbers, and symbols. It can be up to 30 characters.

Note: The router user name and password are not the same as the user name and password for logging in to your Internet connection. See *Types of Logins* on page 28 for more information about login types.

➢ **To change your password or login time-out:**

1. Select **Maintenance > Set Password** to display the following screen:

Set Password

Old Password	
New Password	
Repeat New Password	

Administrator login times out after idle for `5` minutes.

[Apply] [Cancel]

2. Enter the old password.

3. Enter the new password twice.

4. Change the login time-out to a value between 1 and 99 minutes if the default value of 5 minutes does not meet your needs.

The administrator's login to the modem router configuration times out after a period of inactivity to prevent someone else from accessing the router interface when you step away.

5. Click **Apply** to save your changes.

   After changing the password, you are required to log in again to continue the configuration. If you have backed up the modem router settings previously, you should do a new backup so that the saved settings file includes the new password. See *Back Up* on page 60 for information about backing up your network configuration.

Log Out Manually

The router interface provides a Logout command at the bottom of the router menus. Log out when you expect to be away from your computer for a relatively long period of time.

Types of Logins

There are three separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

*   **Router login** logs you in to the router interface. See *Log In to the N600 Modem Router* on page 18 for details about this login.
*   **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
*   **Wi-Fi network name and passphrase** logs you in to your wireless network. This login is preconfigured and can be found on the label on the bottom of your unit. See *Chapter 3, Wireless Settings*, for more information.

Wireless Settings 3

Protecting your wireless network

This chapter contains the following sections:

- *Wireless Adapter Compatibility*
- *Preset Security*
- *Wireless Security Basics*
- *Add Clients (Devices) to Your Network*
- *Wireless Settings*

Wireless Adapter Compatibility

A wireless adapter is the wireless radio in your computer or wireless device that lets it connect to a wireless network. Most computers or wireless devices come with an adapter already installed, but if it is outdated or slow, you can purchase a USB adapter to plug into a USB port.

Make sure the wireless adapter in each computer in your wireless network supports the same security settings as the modem router. See the next section, *Preset Security* for information about the modem router's preconfigured security settings.

> **Note:** If you connect devices to your modem router using WPS as described in *Wi-Fi Protected Setup (WPS) Method* on page 33, those devices assume the security settings of the modem router.

Preset Security

The modem router comes with preset security. This means that the Wi-Fi network name (SSID), passphrase, and security option (encryption protocol) are preset in the factory. You can find the preset SSID and passphrase on the bottom of the unit.

- **Wi-Fi network name (SSID)** identifies your network so devices can find it.
- **Passphrase** controls access to your network. Devices that know the SSID and the passphrase can find your wireless network and connect.

> **Note:** The preset SSID and passphrase are uniquely generated for every device to protect and maximize your wireless security.

- **Security option** is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. The preset security option is WPA-PSK/WPA2-PSK mixed mode, described in *Wireless Security Options* on page 32.

The Wireless Settings screen lets you view and change the preset security settings. ***However, NETGEAR recommends that you not change your preset security settings***. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

Wireless Security Basics

Unlike wired network data, wireless data transmissions extend beyond your walls and can be received by any device with a compatible wireless adapter (radio). For this reason, it is very important to maintain the preset security and understand the other security features available to you. Besides the preset security settings described earlier, your modem router has the security features described here and in *Chapter 4, Content Filtering*.

- Turn off wireless connectivity
- Disable SSID broadcast
- Restrict access by MAC address
- Wireless security options

Turn Off Wireless Connectivity

You can completely turn off the wireless connectivity of the modem router by pressing the Wireless On/Off button on its front panel 🛜. For example, if you use your notebook computer to wirelessly connect to your modem router and you take a business trip, you can turn off the wireless portion of the modem router while you are traveling. Other members of your household who use computers connected to the modem router through Ethernet cables can still use the modem router.

Disable SSID Broadcast

By default, the modem router broadcasts its Wi-Fi network name (SSID) so devices can find it. If you change this setting to not allow the broadcast, wireless devices cannot find your modem router unless they are configured with the same SSID. See *Wireless Access Point Settings* on page 36 for the procedure.

Turning off SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. If you allow the broadcast, be sure to keep wireless security enabled.

Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific computers based on their Media Access Control (MAC) addresses. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the modem router. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed (unencrypted).The Wireless Station Access List determines which wireless hardware devices are allowed to connect to the modem router by MAC address.

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are two types of encryption: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WPA has several options including pre-shared key (PSK) encryption.

This section presents an overview of the security options and provides guidance on when to use which option.

WEP Encryption

WEP uses an old encryption method and can be easily decoded with today's powerful computers. Use this mode only when you have a very old legacy wireless client that does not support WPA-PSK. The Wi-Fi alliance highly recommends against using WEP and plans to make it obsolete. If you do decide to use WEP, see *To set up WEP:* on page 37 for the procedure.

WPA Encryption

WPA encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means the product is authorized by the Wi-Fi Alliance (*http://www.wi-fi.org/*) because it complies with the worldwide single standard for high-speed wireless local area networking. For information about how to use the WPA home options, see *To set up WPA2 or WPA security:* on page 37.

WPA-PSK uses a much stronger encryption algorithm than WEP so it is harder to decode. This option uses a passphrase to perform the authentication and generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards, but not all wireless access points. It is superseded by WPA2-PSK.

WPA2-PSK is the strongest. It is advertised to be theoretically indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is usually implemented through hardware, while WPA-PSK is usually implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

WPS-PSK + WPA2-PSK mixed mode is the preconfigured security mode on the modem router. NETGEAR recommends mixed mode because it provides broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. The product documentation for your wireless adapter and WPA client software should have instructions about configuring their WPA settings.

WPA-802.1x is enterprise-level security and requires an authentication server to recognize and authorize client access. The authentication server is called Remote Authentication Dial In User Service (RADIUS). Every wireless client has a user login on the RADIUS server, and the modem router has a client login on the RADIUS server. Data transmissions are encrypted

with an automatically generated key. For information about how to use the WPA enterprise option, see *To set up WEP:* on page 37.

Add Clients (Devices) to Your Network

Choose either the manual or the WPS method to add wireless devices, including guest devices, and other equipment to your wireless network.

Manual Method

➢ **To add clients (devices) to your network manually:**

1. Open the software that manages your wireless connections on the wireless device (laptop computer, gaming device, iPhone) that you want to connect to your router. This software scans for all wireless networks in your area.

2. Look for your network and select it. If you did not change the name of your network during the setup process, look for the default Wi-Fi network name (SSID) and select it. The default Wi-Fi network name (SSID) is located on the product label on the bottom of the router.

3. Enter the modem router passphrase and click **Connect**. The default modem router passphrase is located on the product label on the bottom of the router.

4. Repeat steps 1–3 to add other wireless devices.

Wi-Fi Protected Setup (WPS) Method

Wi-Fi Protected Setup (WPS) is a standard for easily adding computers and other devices to a home network while maintaining security. To use WPS, make sure that all wireless devices to be connected to the network are Wi-Fi certified and support WPS. During the connection process, the client gets the security settings from the router so that every device in the network has the same security settings.

> **Note:** However, if you find that the router is generating new security settings for each added device, it means that the default value for Keep Existing Wireless Settings has changed. See *WPS Settings* on page 87 for more information about this setting.

All Wi-Fi-certified and WPS-capable products are compatible with the NETGEAR products that have Push 'N' Connect, which is based on WPS.[1] For information about how to view a list of all wireless and wired devices connected to your modem router, see *View Attached Devices* on page 64.

You can use the WPS (Push 'N' Connect) or router interface method to add wireless devices and other equipment to your wireless network. WEP security does not support WPS. If you try to use WPS to connect a WEP device to your network, it cannot connect.
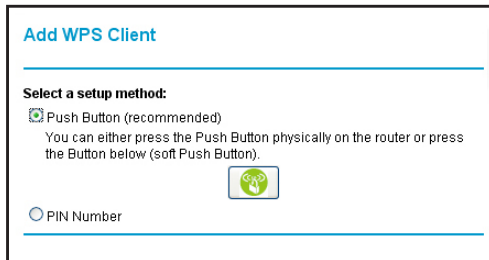
1. For a list of other Wi-Fi-certified products available from NETGEAR, go to http://www.wi-fi.org .

WPS (Push 'N' Connect) Method

➢ **If your wireless device supports WPS (Push 'N' Connect), follow these steps:**

1. Press the **WPS** button on the router front panel .

2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device. The device is now connected to your router.

3. Repeat steps 1–2 to add other WPS wireless devices.

Router Interface Method

➢ **To add clients (devices) using the router interface:**

1. Select **Add WPS Client** at the top of the router menus. If you cannot select Add WPS Client, select **Setup > Wireless Settings** and make sure that WPS is selected.

2. Click **Next**. The following screen lets you select the method for adding the WPS client.
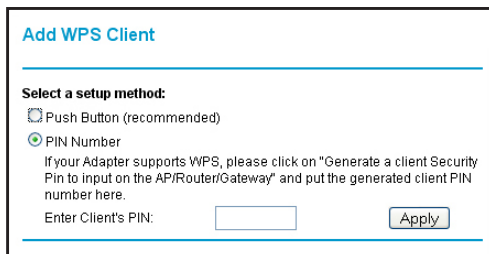
3. Select either **Push Button** or **PIN Number**. With either method, the client wireless device attempts to detect the WPS signal from the modem router and establish a wireless connection in the time allotted.

   The PIN method displays this screen so you can enter the client security PIN number:

   • While the modem router attempts to connect to a WPS-capable device, the WPS LED on the front of the modem router blinks green. When the modem router establishes a WPS connection, the LED is solid green.

   • If a connection is established, the modem router WPS screen displays a confirmation message.

4. Repeat to add another WPS client to your network.

Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network configuration. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

Before you begin, check the following:

- Every wireless computer has to be able to obtain an IP address by DHCP from the router as described in *Use Standard TCP/IP Properties for DHCP* on page 17.
- Each computer or wireless adapter in your network supports the wireless mode (bandwidth/data rate) and the security option you want to use.

➢ **To configure the wireless settings:**

If you use a wireless connection to log in and change the wireless security settings, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the modem router to configure the wireless settings.

1. Select **Setup > Wireless Settings** to display the following screen.

2. Make any changes that are needed, and click **Apply** when done to save your settings.

The screen sections, settings, and procedures are explained in the following sections.

3. After you finish adjusting settings and click Apply, configure and test your computers for wireless connectivity:

    a. set the wireless adapter of your computers to have the same SSID and channel that you specified in the router.

    b. Check that the adapters have a wireless link and can obtain an IP address by DHCP from the modem router.

Wireless Network Settings

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive.

Region. The location where the modem router is used. It might not be legal to operate the modem router in a region other than the regions listed.

Channel. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

Mode. Up to 145 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 65 Mbps supports up to 65 Mbps.

Wireless Access Point Settings

Enable. When this check box is selected, the router accepts wireless clients. When the check box is not selected, the router accepts wired clients only. This check box is selected by default.

Allow Broadcast of Name (SSID). This setting allows the modem router to broadcasts its SSID so wireless stations can see this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear the **Allow Broadcast of Name (SSID)** check box and click **Apply**.

Wireless Isolation. When this check box is selected, wireless stations cannot communicate with each other or with stations on the wired network. This check box is not selected by default.

Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. See *Wireless Security Options* on page 32 for an explanation of the security options and when to use which one.

➢ **To set up WPA2 or WPA security:**

1. In the Security Options sections, select the WPA2 or WPA options that you want.

2. In the Passphrase field that displays when you select a WPA security option, enter the network keys (passphrases) that you want to use. They are text strings from 8 to 63 characters.

➢ **To set up WEP:**

WEP is a legacy security setting. NETGEAR recommends that you use WPA2 or WPA security unless you have legacy wireless equipment that supports only WEP. WEP encryption is available only when the Mode setting is Up to 54 Mbps.

1. In the Security Options section, select **WEP** to display the following screen:

2. Select the authentication type. The default is Automatic. Other choices are Open System (any client can authenticate itself to the network) and Shared Key (a passphrase and a four-way challenge is needed for authentication).

3. Select the encryption strength setting, either 64 bit or 128 bit.

4. Enter the four data encryption keys either manually or automatically. These values have to be identical on all computers and access points in your network.

   - Automatic. Enter a word or group of printable characters in the Passphrase field, and click **Generate**. The four key fields are automatically populated with key values.

- Manual. The number of hexadecimal digits that you enter depends on the encryption strength setting:

    - For 64-bit WEP, enter 10 hexadecimal digits (any combination of 0–9, a–f, or A–F).

    - For 128-bit WEP, enter 26 hexadecimal digits (any combination of 0–9, a–f, or A–F).

5. Select the radio button for the key you want to make active.

   Make sure that you understand how the WEP key settings are configured in your wireless adapter. Wireless adapter configuration utilities such as the one in Windows XP allow one key entry, which has to match the default key you set in the modem router.

6. Click **Save** to save your settings or click **Apply** so your changes to take effect immediately.

Content Filtering

4

Keeping unwanted content out of your network

This chapter explains how to use the basic firewall features of the modem router to prevent objectionable content from reaching the computers and other devices connected to your network.

This chapter contains the following sections:

- *Live Parental Controls*
- *Keyword Blocking of HTTP Traffic*
- *Firewall Rules to Control Network Access*
- *Set the Time Zone*
- *Set the Time Zone*
- *Schedule Firewall Services*
- *Email Logs and Alerts*
- *Log the Network Activity*

Live Parental Controls

The free Live Parental Controls application is available at the NETGEAR website. Use youre web browser to visit *www.netgear.com/lpc*.
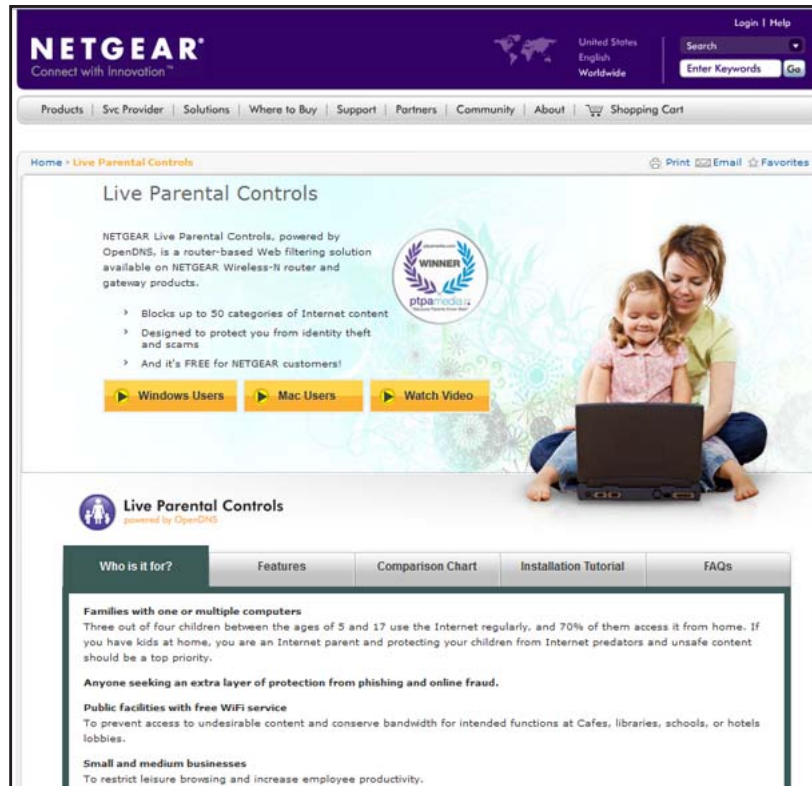
You can learn more about Live Parental Controls or download the application.

Keyword Blocking of HTTP Traffic

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a scheduled.

➢ **To set up keyword blocking:**

1. Select **Content Filtering > Block Sites**.

2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the Keyword field, enter a keyword or domain, click **Add Keyword,** and click **Apply**.

   The Keyword list supports up to 32 entries. Here are some sample entries:
   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.

Delete a Keyword or Domain

➢ **To delete a keyword or domain:**

1. Select the keyword you want to delete from the list.
2. Click **Delete Keyword** and click **Apply** to save your changes.

Specify a Trusted Computer

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

➢ **To specify a trusted computer:**

1. In the **Trusted IP Address** field, enter the IP address.

2. Click **Apply** to save your changes.

Firewall Rules to Control Network Access

By default your router blocks any inbound traffic from the Internet to your computers except for replies to your outbound traffic. You might need to create exceptions to this rule to allow remote computers to access a server on your local network or to allow certain applications and games to work correctly. Your router provides port forwarding and port triggering for creating these exceptions.

This section covers the following topics:

*   *Remote Computer Access Basics*
*   *Port Triggering to Open Incoming Ports*
*   *Port Forwarding to Permit External Host Communications*
*   *How Port Forwarding Differs from Port Triggering*
*   *Configure Port Forwarding to Local Servers*
*   *Configure Port Triggering*

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser and your operating system assigns port number 5678 to this browser session.

2. You type http://www.example.com into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your router.

    Source address. Your computer's IP address.

    Source port number. 5678, which is the browser session.

    Destination address. The IP address of www.example.com, which your computer finds by asking a DNS server.

    Destination port number. 80, which is the standard port number for a web server process.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending the web page request message to www.example.com, your router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):

    *   The source address is replaced with your router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.

    *   The source port number is changed to a number chosen by the router, such as 33333. This is necessary because two computers could independently be using the same session number.

    Your router then sends this request message through the Internet to the web server at www.example.com.

4. The web server at www.example.com composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your router.

    Source address. The IP address of www.example.com.

    Source port number. 80, which is the standard port number for a web server process.

    Destination address. The public IP address of your router.

    Destination port number. 33333.

5. Upon receiving the incoming message, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router then modifies the message to restore the original address information replaced by NAT. Your router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.

    Source address. The IP address of www.example.com.

    Source port number. 80, which is the standard port number for a web server process.

    Destination address. Your computer's IP address.

    Destination port number. 5678, which is the browser session that made the initial request.

6. When you finish your browser session, your router eventually detects a period of inactivity in the communications. Your router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your router from a particular service port number, and replies from the remote computer to your router are directed to that port number. If the remote server sends a reply back to a different port number, your router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies back to multiple port numbers. Using the port

triggering function of your router, you can tell the router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an "identify" message to your computer on port 113. Using port triggering, you can tell the router, "When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer." Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.

2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your router.

3. Your router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.

4. Noting your port triggering rule and having observed the destination port number of 6667, your router creates an additional session entry to send any incoming port 113 traffic to your computer.

5. The IRC server sends a return message to your router using the NAT-assigned source port (as in the previous example, let's say port 33333) as the destination port. The IRC server also sends an "identify" message to your router with destination port 113.

6. Upon receiving the incoming message to destination port 33333, your router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the router restores the original address information replaced by NAT and sends this reply message to your computer.

7. Upon receiving the incoming message to destination port 113, your router checks its session table and learns that there is an active session for port 113, associated with your computer. The router replaces the message's destination IP address with your computer's IP address and forwards the message to your computer.

8. When you finish your chat session, your router eventually senses a period of inactivity in the communications. The router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application, or user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.1.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. The user of a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your router. The remote computer composes a web page request message with the following destination information:

    Destination address. The IP address of www.example.com, which is the address of your router.

    Destination port number. 80, which is the standard port number for a web server process.

    The remote computer then sends this request message through the Internet to your router.

2. Your router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic should be forwarded to local IP address 192.168.1.123. Therefore, your router modifies the destination information in the request message:

    The destination address is replaced with 192.168.1.123.

    Your router then sends this request message to your local network.

3. Your web server at 192.168.1.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your router.

4. Your router performs Network Address Translation (NAT) on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

* Port triggering can be used by any computer on your network, although only one computer can use it at a time.
* Port forwarding is configured for a single computer on your network.
* Port triggering does not need to know the computer's IP address in advance. The IP address is captured automatically.
* Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
* Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
* Port forwarding is always active and does not need to be triggered.

Configure Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

Use the Port Forwarding screen to configure the router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before starting, you need to determine which type of service, application, or game you want to provide, and the local IP address of the computer that provides the service. The server computer has to always have the same IP address.

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your product.

➢ **To configure port forwarding:**

1. Select **Content Filtering > Port Forwarding/Port Triggering** to display the following screen:

2. Select the **Port Forwarding** radio button as the service type.

3. From the Service Name list, select the service or game that you will host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 47.

4. In the corresponding Server IP Address field, enter the last digit of the IP address of your local computer that will provide this service.

5. Click **Add**. The service appears in the list in the screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, you have to first determine which port number or range of numbers is used by the application. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➢ **When you have the port number information, follow these steps:**

1. Select **Content Filtering > Port Forwarding/Port Triggering**.

2. Select the **Port Forwarding** radio button as the service type.

3. Click the **Add Custom Service** button to display the following screen:

4. In the Service Name field, enter a descriptive name.

5. In the Protocol field, select the protocol. If you are unsure, select **TCP/UDP**.

6. In the Starting Port field, enter the beginning port number.
   - If the application uses a single port, enter the same port number in the **Ending Port** field.
   - If the application uses a range of ports, enter the ending port number of the range in the Ending Port field.

7. In the Server IP Address field, enter the IP address of your local computer that will provide this service.

8. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. In the table, select the button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➢ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation. In this example, your router always gives your web server an IP address of 192.168.1.33.

2. In the Port Forwarding screen, configure the router to forward the HTTP service to the local address of your web server at **192.168.1.33**. HTTP (port 80) is the standard protocol for web servers.

3. (Optional) Register a host name with a Dynamic DNS service, and configure your router to use the name. To access your web server from the Internet, a remote user has to know the IP address that has been assigned by your ISP. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetgear.dyndns.org.

Configure Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the router monitors outbound traffic looking for a specified outbound "trigger" port. When the router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

While port forwarding creates a static mapping of a port number or range to a single local computer, port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

> **Note:** If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP).

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To set up port triggering:**

1. Select **Content Filtering > Port Forwarding/Port Triggering** to display the following screen:

2. Select the **Port Triggering** radio button to display the port triggering information.

3. Clear the **Disable Port Triggering** check box.

> **Note:** If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the router is retained even though it is not used.

4. In the Port Triggering Timeout field, enter a value up to 9999 minutes. This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the router cannot be sure when the application has terminated.

Content Filtering

5. Click **Add Service**.

6. In the Service Name field, type a descriptive service name.

7. In the Service User field, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address**, and enter the IP address of one computer to restrict the service to a particular computer.

8. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.

9. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.

10. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.

11. Click **Apply**. The service appears in the Port Triggering Portmap table.

Set the Time Zone

The modem router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

➢ **To set the time zone:**

1. Select **Content Filtering > Schedule** to display the following screen:

2. Select your time zone. This setting determines the blocking schedule and time-stamping of log entries.

3. If your time zone is in daylight savings time, select the **Adjust for Daylight Savings Time** check box to add one hour to standard time.

> **Note:** If your region uses daylight savings time, select Adjust for Daylight Savings Time on the first day and clear it after the last day.

4. The modem router has a list of NETGEAR NTP servers. If you would prefer to use a particular NTP server as the primary server, select the **Use this NTP Server** check box, and enter its IP address.

5. Click **Apply** to save your settings.

Schedule Firewall Services

If you enabled services blocking in the Block Services screen or port forwarding in the Port Forwarding/Port Triggering screen, you can set up a schedule for when blocking occurs or when access is not restricted.

➢ **To schedule firewall services:**

1. Select **Content Filtering > Schedule** to display the following screen:

2. To block Internet services based on a schedule, select **Every Day**, or select one or more days. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter times in the **Start Time** and **End Time** fields.

Note: Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule is effective through midnight the next day.

---

3. Click **Apply** to save your settings.

Email Logs and Alerts

To receive logs and alerts by email, provide your email information in the Email screen, and specify which alerts you want to receive and how often.

➢ **To enable security event email notification:**

1. Select **Content Filtering > Email** to display the following screen:

2. Fill in the fields and click **Apply**.

Email Screen Fields

*   **Turn E-mail Notification On**. Select this check box if you want to receive email logs and alerts from the modem router.

*   **Send To This E-mail Address**. Enter the email address where you want logs and alerts sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.

*   **Outgoing Mail Server**. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.

*   **My Mail Server requires authentication**. If you use an outgoing mail server provided by your current ISP, you do not need to select this check box. If you use an email account that is not provided by your ISP, select this check box, and enter the required user name and password information.

*   **Send E-Mail alerts immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.

- **Send Logs According to this Schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

    - **Day for sending logs** specifies which day of the week to send the log. This is relevant when the log is sent weekly.

    - **Time for sending log** specifies the time of day to send the log. This is relevant when the log is sent daily or weekly.

If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot email the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

Log the Network Activity

A log is a detailed record of the websites that users on your network have accessed or attempted to access. If you have set up content filtering on the Block Sites screen, the Logs screen shows you when someone on your network tried to access a blocked site. If you have email notification on, you receive these logs in an email message. If you do not have email notification set up, you can view the logs on the Logs screen.

➢ **To log the network activity:**

1. Select **Content Filtering > Logs** to display the Logs screen:

    a. To delete all the log entries, click **Clear Log**.

    b. To see the most recent access attempts, click **Refresh**.

    c. To send the log file to your e-mail account, click **Send Log**. This feature is useful for testing your e-mail settings.

2. Use the Include in Log check boxes to determine which events are included in the log. Selecting all check boxes increases the size of the log, so it is good practice to disable any events that are not really required.

- **Attempted access to blocked sites**. If selected, attempted Internet accesses that were blocked are logged.

- **Connections to the Web-based interface of this Router**. If selected, connections are logged to this router, rather than through this router to the Internet.

- **Router operation**. If selected, router operations not covered by the preceding selections are logged.

- **Known DoS attacks and Port Scans**. If selected, denial of service attacks, as well as port scans, are logged.

3. The logs can be sent to a syslog server. Enable one of the three options in the Syslog section, as required:

- **Disable**. Select this if you do not have a syslog server.

- **Broadcast on LAN**. The syslog data is broadcast rather than sent to a specific syslog server. Use this if your syslog server does not have a fixed IP address.

- **Send to this Syslog server IP address**. If your syslog server has a fixed IP address, select this option, and enter the IP address of your syslog server.

4. Click **Apply** to save your changes.

Network Maintenance

5

Administering your network

This chapter describes the modem router settings for administering and maintaining the router and home network.

> **Note:** For security reasons, the modem router has its own user name **admin** and its password that defaults to **password**. You can and should update your password regularly. See *Change Password and Login Time-Out* on page 27.

This chapter contains the following sections:

- *Upgrade the Router Firmware*
- *Manually Check for Firmware Upgrades*
- *Manage Configuration File*
- *View Router Status*
- *View Attached Devices*
- *Run Diagnostic Utilities*

Upgrade the Router Firmware

The modem router firmware (routing software) is stored in flash memory. By default, when you log in to your modem router, it checks the NETGEAR website for new firmware and alerts you if there is a newer version.

⚠️ **WARNING!**

> **When uploading firmware to the modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.**

Automatic Firmware Checking Off

You can turn the automatic firmware checking off and check for firmware updates manually if you prefer. See *Manually Check for Firmware Upgrades* on page 59. To turn off the automatic firmware check at login:

➢ **To turn off automatic firmware checking:**

1. Select **Maintenance > Router Upgrade**.
2. Clear the **Check for Updated Firmware Upon Log-in** check box at the bottom of this screen:

Checking for Firmware Updates

The router is checking the NETGEAR server to see if upda available for your router.

This could take up to 90 seconds, please wait ...

☑ Check for Updated Firmware Upon Log-in

[Cancel]

Automatic Firmware Checking On

When automatic firmware checking is on, the modem router performs the check and notifies you if an upgrade is available or not as shown here.
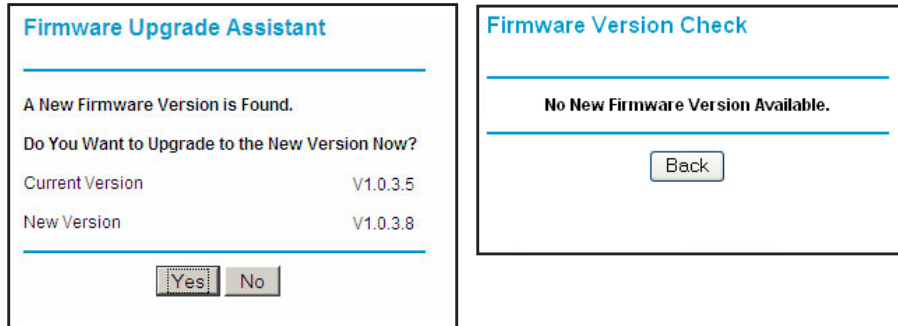
Firmware Upgrade Assistant

A New Firmware Version is Found.

Do You Want to Upgrade to the New Version Now?

Current Version   V1.0.3.5

New Version   V1.0.3.8

Yes   No

Firmware Version Check

No New Firmware Version Available.

Back

Figure 9. Firmware check notification screens

➢ **To turn on automatic firmware checking:**

1. Click **Yes** to allow the modem router to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your modem router restarts.

2. Go to the DGND3800B support page at *http://www.netgear.com/support* and read the new firmware release notes to determine whether you need to reconfigure the modem router after upgrading.

> **Note:** If you get a "Firmware needs to be reloaded" message, it means a problem has been detected with the router's firmware. Follow the prompts to correct the problem, or see *Firmware Needs to Be Reloaded* on page 144 for a description of the steps.

Manually Check for Firmware Upgrades

You can use the Router Upgrade screen to manually check the NETGEAR website for newer versions of firmware for your product.

⚠️ **WARNING!**

When uploading firmware to the modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

➢ **To check for firmware upgrades manually:**

1. Select **Maintenance > Router Status** and make a note of the modem router firmware version number.

2. Go to the DGND3800B support page on the NETGEAR website at *http://www.netgear.com/support.*

3. If the firmware version on the NETGEAR website is newer than the firmware on your modem router, download the file to your computer.

4. Select **Maintenance > Router Upgrade** to display the following screen:

   ```
   Router Upgrade

   Check for New Version from the Internet    [ Check ]

   ☑ Check for New Version Upon Log-in

   Locate and Select the Upgrade File from your Hard Disk:
   [                              ] [ Browse... ]

           [ Upload ]  [ Cancel ]
   ```

5. Click **Browse**, and locate the firmware you downloaded (the file ends in .img).

6. Click **Upload** to send the firmware to the modem router.

   When the upload is done, your modem router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether or not you need to reconfigure the modem router after upgrading.

Manage Configuration File

The router configuration settings are stored in a configuration file (*.cfg). This file can be backed up to your computer, restored, or reverted to factory default settings.

Back Up

➢ **To back up the configuration file:**

1. Select **Maintenance > Backup Settings** to display the following screen:

Backup Settings

Save a copy of current settings

    Save

Restore saved settings from a file

                                Browse...
    Restore

Revert to factory default settings

    Erase

2. Click **Save** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore

➢ **To restore a configuration file:**

1. Enter the full path to the file on your network, or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the modem router.

Upon completion, the modem router reboots.

Erase

Click the **Erase** button to reset the modem router to its factory default settings. Alternately, press the **Wireless On/Off** and **WPS** buttons on the side panel of the modem router simultaneously for 6 seconds.

Erase sets the password to **password** and the LAN IP address to **192.168.0.1**, and enables the modem router's DHCP.

View Router Status

Select **Maintenance > Router Status** to display the Router Status screen:.

You can use the Router Status screen to check the current firmware, settings, and statistics for your router. If something needs to be changed, you have to change it on the relevant screen.

Account Name. This is the account name that you entered in the Setup Wizard or Basic Settings screen.

Firmware Version. This is the current software the router is using. This changes if you upgrade your router.

Internet Port. These are the current settings that you set in the Setup Wizard or Basic Settings screen.

- **MAC Address**. The physical address of the router, as seen from the Internet.
- **IP Address**. Current Internet IP address. If assigned dynamically, and no Internet connection exists, this is blank or 0.0.0.0.
- **Network Type**. Indicates either Client (IP address is obtained dynamically) or None.
- **IP Subnet Mask**. The subnet mask associated with the Internet IP address.
- **Domain Name Server**. Displays the address of the current DNS.

LAN Port. These are the current settings, as set in the LAN IP Setup screen.

- **MAC Address**. The physical address of the router, as seen from the LAN.
- **IP Address**. LAN IP address of the router.
- **DHCP**. Indicates if the router is acting as a DHCP server for devices on your LAN.
- **IP Subnet Mask**. Subnet mask associated with the LAN IP address.

Modem. The current modem status and settings are shown in this section.

- **ADSL Firmware Version**. This is the version number of the low-level ADSL firmware. This is contained within the router firmware.
- **Modem Status**. The current state of the ADSL connection to your phone company.
- **DownStream Connection Speed**. The connection speed of the ADSL connection from the phone company to your router.
- **UpStream Connection Speed**. The connection speed of the ADSL connection from your router to the phone company.
- **VPI**. The VPI setting entered on the ADSL Settings screen.
- **VCI**. The VCI setting entered on the ADSL Settings screen.

Wireless Port. These are the current settings, as set in the Wireless Settings screen.

- **Name** (SSID). SSID of the router.
- **Region**. The location (country).
- **Channel**. The current channel in use.
- **Wireless AP**. Indicates if the access point feature of the router is enabled or not. If not enabled, the Wireless LED on the front panel is off.
- **Broadcast Name**. Indicates if the router is broadcasting its SSID.

To see router performance statistics such as the number of packets sent and number of packets received for each port, click **Show Statistics**.

To see information about your current connection, click **Connection Status**.

Guest Network.

Show Statistics Button

Click the **Show Statistics** button on the Router Status screen to display a screen similar to this:

Figure 10. Router statistics screen

- **Port**. The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:

    - **Status**. The link status of the port.

    - **TxPkts**. The number of packets transmitted since reset or manual clear.

    - **RxPkts**. The number of packets received since reset or manual clear.

    - **Collisions**. The number of collisions since reset or manual clear.

    - **Tx B/s**. The current line utilization—percentage of current bandwidth used.

    - **Rx B/s**. The average line utilization.

    - **Up Time**. The time elapsed since the last power cycle or reset.

- **ADSL Link Downstream or Upstream**. The statistics for the upstream and downstream link. These statistics are of interest to your technical support representative if you have problems obtaining or maintaining a connection.

- **Connection Speed**. Typically, the downstream speed is faster than the upstream speed.

- **Line Attenuation**. The line attenuation increases the farther you are physically located from your ISP's facilities.

- **Noise Margin**. The signal-to-noise ratio, which is a measure of the quality of the signal on the line.

- **Poll Interval**. The interval at which the statistics are updated in this window. Click the **Stop** button to freeze the display.

Connection Status

In the Router Status screen, click the **Connection Status** button to display a screen similar to this:

Figure 11. Connection Status screen

Connection Time. The time elapsed since the last connection to the Internet.

Connecting to sender. The connection status.

Negotiation. Success or Failed.

Authentication. Success or Failed.

Obtaining IP Address. The IP address assigned to the WAN port by the ISP.

Obtaining Network Mask. The network mask assigned to the WAN port by the ISP.

View Attached Devices

The Attached Devices screen presents a table of all IP devices that the modem router has discovered on the local network. Select **Maintenance > Attached Devices** to view the following table:

For each device, the table shows the IP address, device name if available, and the Ethernet MAC address. Note that if the modem router is rebooted, the table data is lost until the modem router rediscovers the devices. To force the modem router to look for attached devices, click the **Refresh** button.

Run Diagnostic Utilities

The modem router has a diagnostics feature that you can use to perform the following functions:

- Ping an IP address to test connectivity to see if you can reach a remote host.
- Perform a DNS lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing table to identify what other modem routers the modem router is communicating with.
- Reboot the modem router to enable new network configurations to take effect or to clear problems with the modem router's network connection.

Select **Maintenance > Diagnostics** to display the following screen.

USB Storage

6

Adding removable storage to your network

This chapter describes how to access and configure a USB storage drive attached to your modem router. The USB ports on the modem router can be used only to connect USB storage devices like flash drives or hard drives. Do not connect computers, USB modems, printers, CD drives, or DVD drives to the these USB ports.

Figure 12. USB ports, front and rear panel

This chapter includes the following sections:

- *USB Drive Requirements*
- *ReadySHARE Access*
- *File-Sharing Scenarios*
- *USB Storage Basic Settings*
- *Edit a Network Folder*
- *USB Storage Advanced Settings*
- *Safely Remove USB Drive*
- *Media Server Settings*
- *Approved USB Devices (Advanced USB Settings)*
- *Connect to the USB Drive with Microsoft Network Settings*

USB Drive Requirements

The modem router works with 1.0 and 1.1 (USB Full Speed) and 2.0 (USB High Speed) standards. The approximate USB bus speeds are shown in the following table.

Table 2. USB Bus Speeds

Bus	Speed/Second
USB 1.1	12 Mbits
USB 2.0	480 Mbits

Actual bus speeds can vary, depending on the CPU speed, memory, speed of the network, and other variables. The modem router should work with USB 2.0-compliant or 1.1-compliant external flash and hard drives. For the most up-to-date list of USB drives supported by the modem router, go to:

http://kbserver.netgear.com/readyshare.

When selecting a USB device, bear in mind the following:

- The USB port on the modem router can be used with one USB hard drive at a time. Do not attempt to use a USB hub attached to the USB port.

- According to the USB 2.0 specification, the maximum available power is 5V @ 0.5A. Some USB devices might exceed this requirement, in which case the device might not function or might function erratically. Check the documentation for your USB device to be sure.

- The modem router supports FAT, FAT32, and NTFS (read only) file systems.

ReadySHARE Access

Once you have set up your modem router, you can connect any USB storage device and share the contents with other users on your network.

You can access your USB device in any of the following ways:

- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, select **Start > Run**, and enter **\\readyshare** in the dialog box. Click **OK**.

- On Windows 7, Windows XP, Windows Vista, and Windows 2000 systems, open Internet Explorer or Safari, and enter **\\readyshare** in the address bar.

- On Mac OS X (version 10.2 or later), enter **smb://readyshare** in the address bar.

- In My Network Places, enter **\\readyshare** in the address bar.

File-Sharing Scenarios

You can share files on the USB drive for a wide variety of business and recreational purposes. The files can be any PC, Mac, or Linux file type including text files, Word, PowerPoint, Excel, MP3, pictures, and multimedia. USB drive applications include:

- Sharing multimedia with friends and family such as MP3 files, pictures, and other multimedia with local and remote users.
- Sharing resources on your network. You might want to store files in a central location so that you do not have to power up a computer to perform local sharing. In addition, you can share files between Macintosh, Linux, and PC computers by using the USB drive as a go-between across the systems.
- Sharing files such as Word documents, PowerPoint presentations, and text files with remote users.

A few common uses are described in the following sections.

Sharing Photos

You can create your own central storage location for photos and multimedia. This eliminates the need to log in to (and pay for) an external photo-sharing site.

➢ **To share files with your friends and family:**

1. Insert your USB drive into the USB port on the modem router either directly or with a USB cable.

   Computers on your local area network (LAN) can automatically access this USB drive using a web browser or Microsoft Networking.

2. If you want to specify read-only access or to allow access from the Internet, see *Approved USB Devices (Advanced USB Settings)* on page 75.

Storing Files in a Central Location for Printing

This scenario is for a family that has one high-quality color printer directly attached to a computer, but not shared on the local area network (LAN). This family does not have a print server.

- One family member has photos on a Macintosh computer that she wants to print.
- The photo-capable color printer is directly attached to a PC, but not shared on the network.
- The Mac and PC are not visible to each other on the network.

➢ **To print photos from a Mac on the printer attached to a PC:**

1. On the Mac, access the USB drive by typing **\\readyshare** in the address field of a web browser. Then copy the photos to the USB drive.

2. On the PC, use a web browser or Microsoft Networking to copy the files from the USB drive to the PC. Then print the files.

Sharing Large Files over the Internet

Sending files that are larger than 5 MB can pose a problem for many email systems. The modem router allows you to share very large files such as PowerPoint presentations or .zip files over the Internet. FTP can be used to easily download shared files from the modem router.

Sharing files with a remote colleague involves the following considerations:

- There are two user accounts: admin and guest. The password for admin is the same one that you use to access the modem router. By default, it is **password**. The guest user account has no password.

- On the FTP site, the person receiving the files should use the guest user account and enter any password (FTP requires that you type something in the password field).

- Be sure to select the **FTP (via Internet)** check box in the USB Storage Advanced Settings screen. This option supports both downloading and uploading of files.

> **Note:** You can enable the HTTP (via Internet) option on the Advanced USB Storage screen to share large files. This option supports downloading files only.

USB Storage Basic Settings

You can view or edit basic settings for the USB storage device attached to your modem router. Select **USB > Basic Settings**. The following screen displays:

If you logged in to the modem router before you connected your USB device, you might not see your USB device in the modem router screens until you log out and then log in again. This screen includes the following fields and buttons:

- **Network Device Name**. The default is \\readyshare. This is the name used to access the USB device connected to the modem router.

- **Folder Name**. Full path of the used by the Network folder.

- **Volume Name**. Volume name from the storage device (either USB drive or HDD).

- Total/Free Space. Shows the current utilization of the storage device.

- **Share Name**. You can click the name shown, or you can type it in the address field of your Web browser.

  If Not Shared is shown, then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.

- **Read/Write Access**. Shows the network folder permissions and access controls.

  - All no password allows all users to access the network folder.

  - admin uses the same password that you use to log in to the modem router.

- **Edit**. You can click the **Edit** button to edit the Available Network folder settings. See *Edit a Network Folder* on page 71.

- **Safely Remove USB Device**. Click this button to safely remove the USB device attached to your modem router. See *Safely Remove USB Drive* on page 74.

➢ **To access a USB device attached to the modem router USB port:**

1. Select **USB > Basic Settings**. The following screen displays:

USB Storage (Basic Settings)

Network/Device Name: \\readyshare

Available Network Folders

Shared Name	Read Access	Write Access	Folder Name	Volume Name	Total Space	Free Space
\\readyshare\USB_Storage	All - no password	All - no password	U:\	HP v100w	1911MB	914MB

Edit

Safely Remove USB Device

Refresh

By default, the USB device is available to all computers on your local area network (LAN).

2. To access your USB device, click the share name or type **\\readyshare** in the address field of your Web browser.
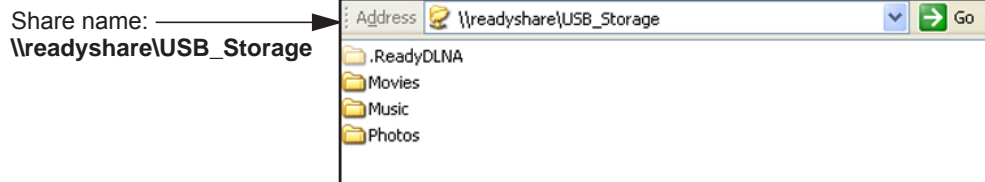
Network/device name: ⎯⎯
**\\readyshare**

Share name: ⎯⎯
\\readyshare\USB_Storage

If you logged in to the modem router before you connected your USB device, you might not see your USB device in the modem router screens until you log out and then log in again.

Edit a Network Folder

You can use the Edit button on either the USB Storage (Basic Settings) or USB Storage (Advanced Settings) screen.

➢ **To edit a network folder:**

1. Select **USB > Advanced Settings**. The USB Storage (Advanced Settings) screen displays:
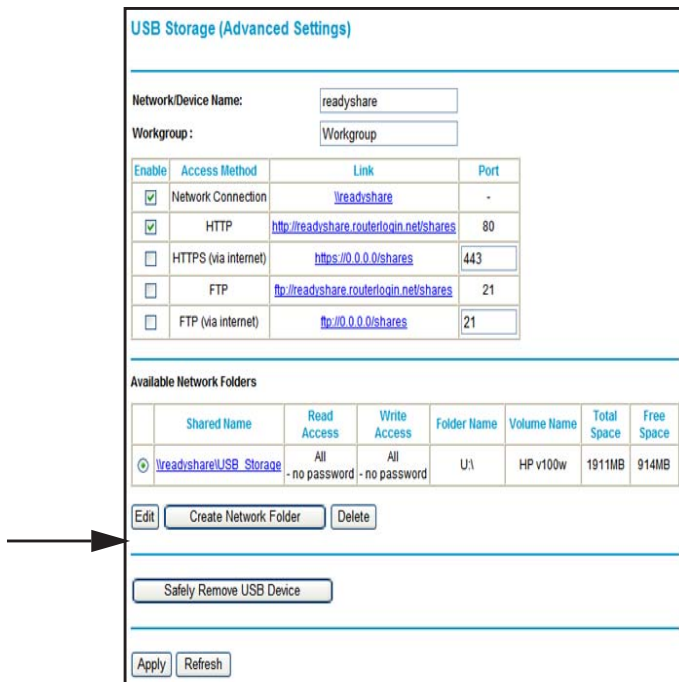
2. Click the **Edit** button

3. Click **Apply** for your changes to take effect.

USB Storage Advanced Settings

To view or change advanced USB settings, select **USB > Advanced Settings**. The USB Storage (Advanced Settings) screen displays:

You can use this screen to specify access to the USB storage device. The settings are as follows:

- **Network Device Name**. The default is readyshare. This is the name used to access the USB device connected to the modem router from your computer.

- **Workgroup**. If you are using a Windows Workgroup rather than a domain, the workgroup name is displayed here.

Access Method

- **Network Connection**. Enabled by default, this allows all users on the LAN to have access to the USB drive.

- **HTTP**. Disabled by default. If you enable this setting, you can type **http://readyshare** to access the USB drive.

- **HTTP (via Internet)**. Disabled by default. If you enable this settings, remote users can type **http://readyshare** to access the USB drive over the Internet.

- **FTP**. Disabled by default.

- **FTP (via Internet)**. Disabled by default. If you enable this settings, remote users can access the USB drive via FTP over the Internet.

Available Network Folders

- **Folder Name**. Full path of the Network folder.
- **Volume Name**. Volume name from the storage device (either USB drive or HDD).
- **Total Free Space**. The space currently available on the storage device.
- **Share Name**. You can click the name shown or you can type it into the address field of your Web browser. If Not Shared is shown, then the default share has been deleted and no other share for the root folder exists. Click the link to change this setting.
- **Read/Write Access**. Shows the permissions and access controls on the Network folder. Selecting **All no password** allows all users to access the Network folder. You are prompted to enter the same password that you use to log in to the modem router.

Create a Network Folder

You can create a network folder on the USB device that is attached to the USB port on the rear panel of the modem router.

➢ **To create a network folder:**

1. From the USB Storage (Advanced Settings) screen, click the **Create Network Folder** button to open the Create a Network Folder screen:

2. Type a name in the Folder field.
   - You can specify the folder's share name, read access, and write access from All-no password to admin.
   - The password for admin is the same one that is used to log in to the modem router . By default it is password.
3. Click **Apply** so that your changes take effect.

Safely Remove USB Drive

To unmount a USB disk drive so that no users can access it, from the USB Settings screen, click the **Safely Remove USB** button. This takes the drive offline.

> ⚠️ **CAUTION:**
>
> Unmount the USB drive before physically unplugging it from the modem router. If the USB disk is removed or a cable is pulled while data is being written to the disk, it could result in file or disk corruption.

Media Server Settings

You can set up the modem router to work with compatible media adapters. Select **USB Storage > Media Servers** to display the following screen:

Enable Media Server. If this feature is enabled, the DGN2200v3 can be located by compatible media adapters, using the UPnP AV standard developed by Intel and its partners. Media content on the DGN2200v3 (in the Content Directories that you specify) can then be accessed and played by the media adapters.

Server Name. The name of the media server that is displayed on client devices. Note that some special characters (such as " / \ [ ] : ; |= , + * ? < > ` ( ) # $ %) and 2-byte characters cannot be used in the server name.

Content Directory. Specify the directories (folders) that the media server should scan for media content. You can specify up to four. Click the **Browse** button to locate and select the folder you want. Each directory can be limited to a certain media type. The default setting scans for all content types. Note that some special characters (such as " \ : * ? < > | ' `) cannot be used in the folder names.

Approved USB Devices (Advanced USB Settings)

You can specify which USB devices are approved for use when connected to the modem router.

➢ **To allow only approved USB devices to be accessed:**

1. Select **Advanced > USB Settings**.

2. Click **Approved Devices**.

3. On the USB Drive Approved Devices screen, select the USB device from the Available USB Devices list.

4. Click **Add**.

5. Select the **Allow only approved devices** check box.

6. Click **Apply** so that your change takes effect.

If you want to approve another USB device, you have to first use the **Safely Remove USB Device** button to unmount the currently connected USB device. Connect the other USB device, and then repeat this process.

Connect to the USB Drive from a Remote Computer

To connect to the USB drive from remote computers using a Web browser, you use the modem router's Internet port IP address.

➢ **To connect to the modem router's USB drive using a Web browser:**

1. First, locate the Internet port IP address. You can view this in the Router Status screen.

   a. Select **Maintenance > Router Status**.

   b. Record the IP address that is listed for the Internet port. This is the IP address you can use to connect to the modem router remotely.

2. Use a web browser to connect to the modem router by typing **ftp://** and the Internet port IP address in the address field.

   For example, type **ftp://10.1.65.4**. If you are using Dynamic DNS, you can type the DNS name rather than the IP address.

3. Type the name and password of the account that has access rights to the USB drive.

   The directories of the USB drive that your account has access to display, for example, share/partition1/directory1. You can now read and copy files from the USB directory.

Connect to the USB Drive with Microsoft Network Settings

You can access the USB drive from local computers on your home or office network using Microsoft network settings. You have to be running Microsoft Windows 2000, XP, or older versions of Windows with Microsoft networking enabled. You can use normal Explorer operations such as dragging and dropping, opening files, or cutting and pasting files from:

• Microsoft Windows Start menu, Run option

• Windows Explorer

• Network Neighborhood or My Network Place

Enabling File and Printer Sharing

Each computer's network properties have to be set to enable network communication with the USB drive. File and Printer Sharing for Microsoft networking have to be enabled, as described in the following sections.

Note: In Windows 2000 and Windows XP, File and Printer Sharing is enabled by default.

Configuring Windows 98SE and Windows ME

The easiest way to get to your network properties is to go to your desktop, right-click **Network Neighborhood** and then select **Properties**. File and Printer Sharing for Microsoft Windows should be listed. If not, click **Add** and follow the installation prompts.

> **Note:** If you have any questions about File and Printer Sharing, contact Microsoft for assistance.

Configuring Windows 2000 and Windows XP

Right-click the network connection for your local area network. File and Printer Sharing for Microsoft Windows should be listed. If not, click **Install** and follow the installation prompts.

Advanced Settings

Configuring for unique situations

<div align="right">

7

</div>

This chapter describes the advanced features of your modem router. The information is for users with a solid understanding of networking concepts who want to set the router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

This chapter contains the following sections:

- *WAN Setup*
- *Dynamic DNS*
- *LAN Setup*
- *Set Up Quality of Service (QoS)*
- *Advanced Wireless Settings*
- *Wireless Repeating Networks*
- *Remote Management*
- *Static Routes*
- *Universal Plug and Play*
- *Traffic Meter*

Note: The Advanced USB Settings feature is in *Chapter 6, USB Storage*.

WAN Setup

➢ **To make changes to the WAN setup:**

1. Select **Advanced > WAN Setup** to display the following screen:

2. Enter the LAN Setup configuration and click **Apply** to save your changes.

> **Note:** The default values work for most users.

WAN Preference

Configure whether the modem router uses only one WAN port exclusively (either ADSL WAN or Ethernet WAN) or detects automatically the WAN port to use.

Disable Port Scan and DOS Protection

The firewall protects your LAN against port scans and denial of service (DOS) attacks. This protection should be disabled only in special circumstances.

Default DMZ Server
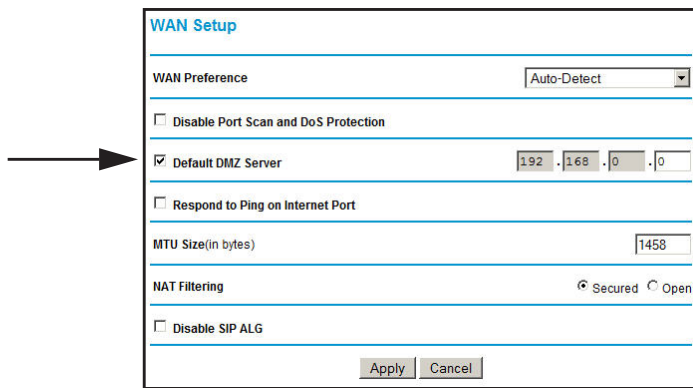
The default demilitarized zone (DMZ) server feature is helpful when you use online games and video conferencing applications that are incompatible with NAT. The modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

Note: For security reasons, you should avoid using the default DMZ server feature. When a computer is designated as the default DMZ server, it loses much of the protection of the firewall and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is usually discarded by the modem router unless the traffic is a response to one of your local computers or a service that you have configured in the Ports screen. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the default DMZ server.

➢ **To assign a computer or server to be a default DMZ server:**

1. In the **WAN Setup** screen, select the **Default DMZ Server** check box.

2. Type the IP address for that server and click **Apply**.

Respond to Ping on Internet Port

If you want the modem router to respond to a ping from the Internet, select this check box. This should be used only as a diagnostic tool, because it allows your modem router to be discovered, which can be a security problem. Do not select this check box unless you have a specific reason to do so.

MTU Size (in bytes)

The normal maximum transmission unit (MTU) value for most Ethernet networks is 1500 bytes, 1492 bytes for PPPoE connections, and 1458 for PPPoA connections. For some ISPs you might need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

NAT Filtering

This option determines how the router deals with inbound traffic. The Secured option provides a secured firewall to protect the computers on LAN from attacks from the Internet, but it might cause some Internet games, point-to-point applications, and multimedia applications no work. The Open option, on the other hand, provides a much less secured firewall, while it allows almost all Internet applications to work.

Disable SIP ALG

The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. The Disable SIP ALG check box allows you to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you do not know in advance what your IP address is, and the address can change frequently. In this case, use a commercial Dynamic DNS service that lets you register your domain to its IP address and forwards traffic directed at your domain to your frequently changing IP address.

The router has a client that can connect to a Dynamic DNS service provider. Once you have configured your ISP account information in the router, whenever your ISP-assigned IP address changes, your router contacts your Dynamic DNS service provider, logs in to your account, and registers your new IP address.

➢ **To enable dynamic DNS:**

1. Select **Advanced > Dynamic DNS** to display the following screen.

2. Access the website of one of the Dynamic DNS service providers whose names appear in the **Service Provider** drop-down list, and register for an account. For example, for dyndns.org, go to www.dyndns.org.

3. Select the **Use a Dynamic DNS Service** check box.

4. Select the name of your Dynamic DNS service provider.

5. Type the host name that your Dynamic DNS service provider gave you. The Dynamic DNS service provider might call this the domain name. If your URL is myName.dyndns.org, then your host name is myName.

6. Type the user name for your Dynamic DNS account.

7. Type the password (or key) for your Dynamic DNS account.

8. If your Dynamic DNS provider allows the use of wildcards in resolving your URL, you can select the **Use Wildcards** check box to activate this feature. For example, the wildcard feature causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org.

9. Click **Apply** to save your settings.

Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the Dynamic DNS service does not work because private addresses are not routed on the Internet.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as DHCP and Routing Information Protocol (RIP). The modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem router's default LAN IP configuration is as follows:

*   **LAN IP address**. 192.168.0.1
*   **Subnet mask**. 255.255.255.0

These addresses are part of the private address range designated by the Internet Engineering Task Force (IETF *http://www.ietf.org/*) for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in the LAN IP Setup screen.

Note: If you change the LAN IP address of the modem router while connected through the browser, you are disconnected. To reconnect, open a new connection to the new IP address and log in.

➢ **To change the LAN settings:**

1. Select **Advanced > LAN Setup**.

LAN Setup

| Device Name | DGND3700 |

LAN TCP/IP Setup

☐ Use Auto IP

IP Address   192 . 168 . 0 . 1

IP Subnet Mask   255 . 255 . 255 . 0

☑ **Use Router as DHCP Server**

Starting IP Address   192 . 168 . 0 . 2

Ending IP Address   192 . 168 . 0 . 254

Address Reservation

| # | IP Address | Device Name | MAC Address |

Add   Edit   Delete

Apply   Cancel

2. Enter the LAN Setup configuration and click **Apply** to save your changes.

Note: The default DHCP and TCP/IP values work for most users.

- **Device Name**. This is an abbreviated name of the modem router. You see this name for the router in Network Explorer on Windows systems.

- **Use Auto IP**. Select this check box if you want the modem router to set up the **LAN IP** addresses automatically.

- **IP Address**. The LAN IP address of the modem router.

- **IP Subnet Mask**. The LAN subnet mask of the modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or modem router.

- **Use Router as DHCP Server**. By default, the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the modem router's LAN. The assigned default gateway address is the LAN address of the router. IP addresses are assigned to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

  For most applications, the default DHCP and TCP/IP settings of the router are satisfactory.

- **Reserved IP Addresses Setup**. When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the router's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

➢ **To reserve an IP address:**

1. Select **Advanced > LAN Setup** and click the **Add** button.

2. In the **IP Address** field, type the IP address to assign to the computer or server. Choose an IP address from the router's LAN subnet, such as 192.168.0.x.

3. Type the MAC address of the computer or server.

> **Tip:** If the computer is already present on your network, copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

> **Note:** The reserved address is not assigned until the next time the computer contacts the router's DHCP server. Reboot the computer or access its IP configuration to force a DHCP release and renew.

➢ **To edit or delete a reserved address entry:**

1. Select the radio button next to the reserved address that you want to edit or delete.

2. Click **Edit** or **Delete**.

Set Up Quality of Service (QoS)

Quality of Service (QoS) is an advanced feature that can be used to prioritize some types of traffic ahead of others. The modem router can provide QoS prioritization over the wireless link and on the Internet connection.

The modem router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application has to be WMM enabled. Legacy applications that do not support WMM, and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

Configure QoS for Internet Access

To specify prioritization of traffic, you have to add or create a policy for the type of traffic.

➢ **To configure QoS for Internet access:**

1. Select **Advanced > QoS Setup**.

QoS Setup

☑ Enable WMM (Wi-Fi multimedia) settings

☐ Turn Internet Access QoS On

☐ Turn Bandwidth Control On

    Uplink bandwidth: Maximum `256` `Kbps ▾`

    Check for current Internet uplink bandwidth `Check`

QoS Priority Rule list   `Setup QoS rule`

`Apply` `Cancel`

2. Click **Setup QoS rule**. The QoS Priority Rule list displays:

QoS Priority Rule list

	#	QoS Policy	Priority	Description
○	1	MSN Messenger	High	MSN Messenger application
○	2	Yahoo Messenger	High	Yahoo Messenger application
○	3	IP Phone	Highest	IP Phone application
○	4	Vonage IP Phone	Highest	Vonage IP Phone application
○	5	NetMeeting	High	NetMeeting application
○	6	AIM	High	AIM application
○	7	Google Talk	Highest	Google Talk application
○	8	Netgear EVA	Highest	NETGEAR EVA application
○	9	SSH	High	SSH application
○	10	Telnet	High	Telnet application
○	11	VPN	High	VPN application

3. To change a rule, select its radio button.

4. Scroll down to the bottom of the screen:

`Edit` `Delete` `Delete All`

`Add Priority Rule`

`Apply` `Cancel`

5. To edit a rule, click **Edit**. To add a custom rule, click **Add Priority Rule**.

6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

7. In the QoS Setup screen, click **Apply**.

Advanced Wireless Settings

➤ **To configure the advanced wireless settings:**

1. Select **Advanced > Wireless Settings** to display the following screen:

The WPS Settings section is not displayed if you selected WEP as the security option.

2. If you make changes, click **Apply**. Note that more settings are available in the Wireless Settings screen. See *Wireless Settings* on page 35.

Note: The modem router is already configured with the optimum advance wireless settings. Do not alter these settings unless directed by NETGEAR support. Incorrect settings might disable the modem router unexpectedly.

Wireless Advanced Settings

Enable Wireless Router Radio. The wireless access point of this router can be enabled or disabled to allow wireless access. The Wireless LED on the front of the router also displays the current status of the wireless access point to let you know if it is disabled or enabled. If it is enabled, wireless stations can access the Internet. If it is disabled, wireless stations cannot access the Internet.

Enable SSID Broadcast. If this feature is enabled, the modem router broadcasts its name (SSID) to all wireless stations. Stations that have no SSID (or a null value) can then adopt the correct SSID for connections to this access point.

Fragmentation Threshold, **CTS/RTS Threshold**, and **Preamble Mode**. Do not change these settings. The Fragmentation Threshold, CTS/RTS Threshold, and Preamble Mode settings are reserved for wireless testing and advanced configuration only.

WPS Settings

Router's PIN. The PIN number that you use on a registrar (for example, from the Network Explorer on a Vista Windows PC) to configure the modem router's wireless settings through WPS. You can also find the PIN on the modem router's product label.

Disable Router's PIN. The PIN function might temporarily be disabled when the modem router detects suspicious attempts to break into the modem router's wireless settings by using the modem router's PIN through WPS. You can manually enable the PIN function by clearing the Disable Router's PIN check box.

Keep Existing Wireless Settings. By default, the Keep Existing Wireless Settings check box is selected. This shows whether the router is in the WPS configured state.

If the Keep Existing Wireless Settings check box is not selected, adding a new wireless client changes the router's wireless settings to an automatically generated random SSID and security key. NETGEAR does not recommend this. In addition, if this option is selected, some external registrars (e.g., Network Explorer on Vista Windows) might not see the router.

Configuring the basic wireless settings from the router's management interface selects this option automatically.

Wireless Card Access List. By default, any wireless computer that is configured with the correct SSID is allowed access to your wireless network. For increased security, you can restrict access to the wireless network to allow only specific computers based on their MAC addresses. On the Wireless Settings screen, select **Setup Access List** to display the Wireless Access List screen.

Wireless Station Access List Settings

The Wireless Stations Access List lets you restrict access to your network to a specific list of devices based on their MAC addresses. This section explains how to set up the list.

➢ **To set up the wireless station access list:**

1. On the Wireless Settings screen, click the **Setup Access List** button to display the Wireless Station Access List screen:

2. Select the **Turn Access Control On** check box to enable access restriction by MAC address.

3. In the Add New Station Manually section, click **Add** to add your computer's MAC address so you do not lose your wireless connection when you click Apply. If you lose your wireless connection, you have to access the modem router from a wired computer or from a wireless computer that is on the access control list.

4. If a wireless station that you want to add to the Trusted Wireless Stations list is connected to the network, select it from the Available Wireless Stations list and click **Add**.

5. If the wireless station is not currently connected, you can enter its address manually. The MAC address is usually printed on the wireless card, or it might appear in the modem router's DHCP table. The MAC address is 12 hexadecimal digits.

   You can also copy and paste the MAC addresses from the modem router's Attached Devices screen (see *View Attached Devices* on page 64) into the MAC Address field. To do this, configure each wireless computer to obtain a wireless link to the modem router. The computer should then appear in the Attached Devices screen.

6. Click **Apply** to save your settings and return to the Wireless Settings screen.

Wireless Repeating Networks

Note: If you want to use the Wireless Repeating feature, you have to go to the Wireless Settings screen and change the wireless security setting of the router to WEP or None, and you have to change the Channel field to a different setting than Auto, which is the default. For more information, see *Wireless Settings* on page 35.

With the modem router, you can build large bridged wireless networks that form an IEEE 802.11n Wireless Distribution System (WDS). Using the modem router with other access points (APs) and wireless devices, you can connect clients using their MAC addresses rather than IP addresses. Here are some examples of wireless bridged configurations:

- **Point-to-point bridge**. The modem router communicates with another bridge-mode wireless station. See *Set Up a Point-to-Point Bridge* on page 90.

- **Multi-point bridge**. The modem router is the "master" for a group of bridge-mode wireless stations. Then all traffic is sent to this master, rather than to other access points. See *Set Up a Multi-Point Bridge* on page 92.

- **Repeater with wireless client association**. Sends all traffic to the remote access point. See *Repeater with Wireless Client Association* on page 93.

The wireless bridging and repeating feature uses the default security profile to send and receive traffic.

Select **Advanced > Wireless Repeating Function** to display the following screen:

- **Enable Wireless Repeating Function**. Select this check box if you want to use the wireless repeating function.

- **Disable Wireless Client Association**. If your modem router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

    - If you are setting up a point-to-point bridge, select this check box.

    - If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

- **Wireless MAC of this router**. This field displays the MAC address for your modem router for your reference. You will need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.

- **Wireless Repeater**. If your modem router is the repeater, select this check box.

- **Repeater IP Address**. If your modem router is the repeater, enter the IP address of the other access point.

- **Base Station MAC Address**. If your modem router is the repeater, enter the MAC address for the access point that is the base station.

- **Wireless Base Station**. If your modem router is the base station, select this check box.

- **Disable Wireless Client Association**. If your modem router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

- **Repeater MAC Address (1 through 4)**. If your modem router is the base station, it can act as the "parent" of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

Set Up a Point-to-Point Bridge

In point-to-point bridge mode, the modem router communicates as an access point with another bridge-mode wireless station. As a bridge, wireless client associations are disabled.

Only wired clients can be connected. Use wireless security to protect this communication. The following figure shows an example of point-to-point bridge mode.
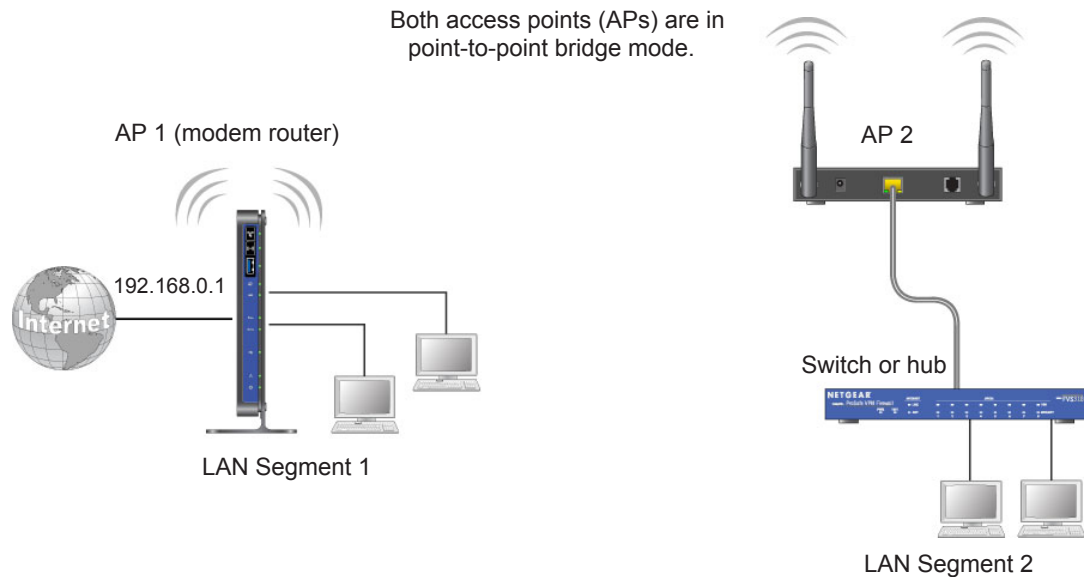

Figure 13. Point-to-point bridge example

➢ **To set up a point-to-point bridge configuration:**

1. Set up your modem router (AP 1) on LAN Segment 1 in point-to-point bridge mode.

   a. In the Wireless Repeating Function screen, select the **Enable Wireless Repeating Function** check box.

   b. Select either the **Wireless Repeater** or **Wireless Base Station** radio button.

   c. Select the corresponding **Disable Wireless Client Association** check box.

   d. Enter the MAC address for the other access point in the bridge. Depending on your selection in step a, use either the Base Station MAC Address field or the Repeater MAC Address 1 field.

   e. Click **Apply**.

2. Set up the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.

   If your modem router is the repeater, then set up AP 2 as the base station; otherwise set up AP 2 as the repeater.

3. Set up both access points and verify that they use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.

4. Disable the DHCP server on AP 2. AP 1 will then be the DHCP server.

5. Verify connectivity across LAN Segment 1 and LAN Segment 2. A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

Set Up a Multi-Point Bridge

Multi-point bridge mode allows a router to bridge to multiple peer access points simultaneously. Wireless client associations are disabled. Only wired clients can be connected.
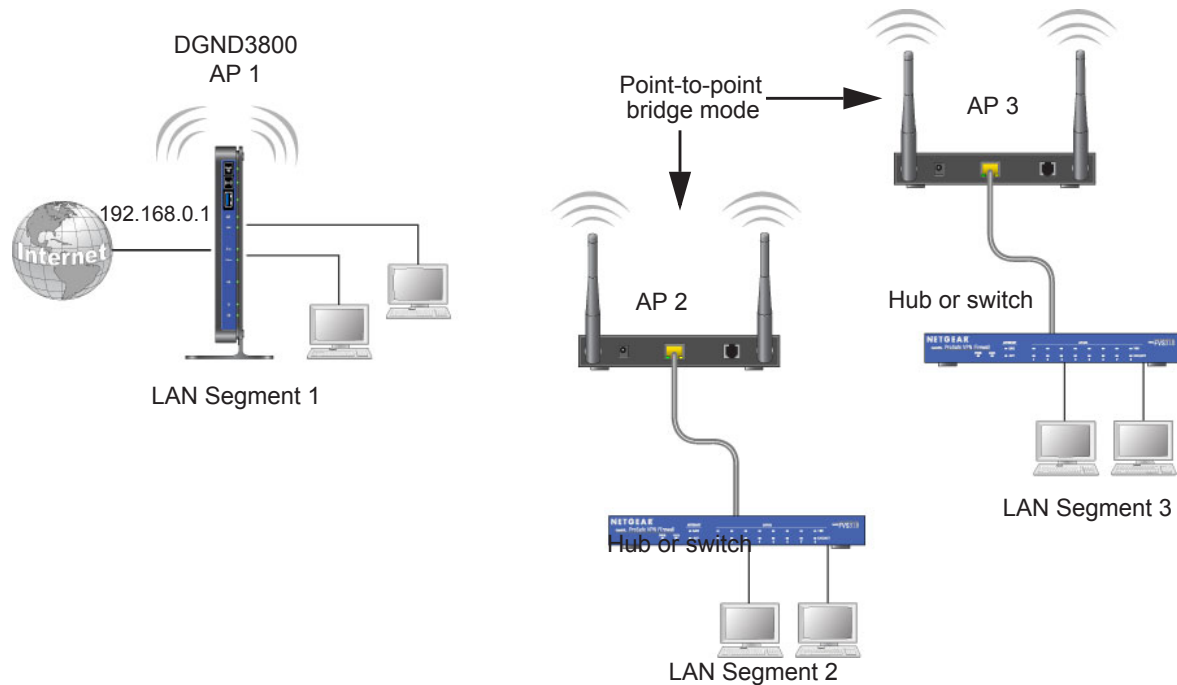

Figure 14. Multi-point bridge example

Multi-point bridge mode configuration includes the following steps:

- Set up the modem router for wireless repeating as the base station, and specify the MAC addresses of the access points that are repeaters.
- Set up the other access points for wireless repeating as repeaters, and specify the MAC address of the modem router as the base station.
- Use wireless security to protect this traffic.

➢ **To set up the multi-point bridge configuration:**

In this example, the modem router is AP 1 on LAN Segment 1 because it is in a central location.

1. Set up your modem router to be the base station in the bridge.

    a. In the Wireless Repeating Function screen for your modem router, select the **Enable Wireless Repeating Function** check box.

    b. Select the **Wireless Base Station** radio button.

    c. Select the corresponding **Disable Wireless Client Association** check box.

    d. Enter the MAC address for the other access points in the bridge in the Repeater MAC Address 1 and Repeater MAC Address 2 fields.

    e. Click **Apply**.

2. Set up AP 2 and AP 3 to be wireless repeaters.

    a. In the Wireless Repeating Function screen for AP 2 and AP 3, select the **Enable Wireless Repeating Function** check box.

    b. Select the **Wireless Repeater** radio button.

    c. Select the corresponding **Disable Wireless Client Association** check box.

    d. Enter the MAC addresses for your modem router in the Base Station MAC Address field.

    e. Click **Apply**.

3. Disable the DHCP server on AP 2 and AP 3. AP 1 will then be the DHCP server.

4. Verify the following for all access points:

- The modem router and other access points operate in the same LAN network address range as the LAN devices.

- Only one access point, your modem router in *Figure 14, Multi-point bridge example*, is set up as the base station. The others are set up as repeaters.

- All access points, including your modem router, are on the same LAN. That is, all the access point LAN IP addresses are in the same network.

- If you are using DHCP, all access points should be set as DHCP clients. This setting is **Obtain an IP address automatically (DHCP Client)** in the Basic Settings screen.

- All access points, including your modem router, use the same SSID, channel, authentication mode, if any, and WEP security settings if security is in use.

5. Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.

    Note: Wireless stations configured as in *Figure 13* on page 91 cannot connect to the modem router or access points. If you want wireless stations to access any LAN segment, use additional access points in any LAN segment.

Repeater with Wireless Client Association

In the repeater mode with wireless client association, your modem router sends all traffic to a base station access point. You can set up the modem router as either the base station (parent) or as the repeater (child) access point.

Note that the following restrictions apply:

- You *do not* have the option of disabling client associations with this modem router.

- You cannot configure a sequence of parent-child APs. You are limited to only one parent access point, although if your modem router is the parent access point, it can connect with up to four child access points.

The following figure shows an example of a repeater mode configuration.
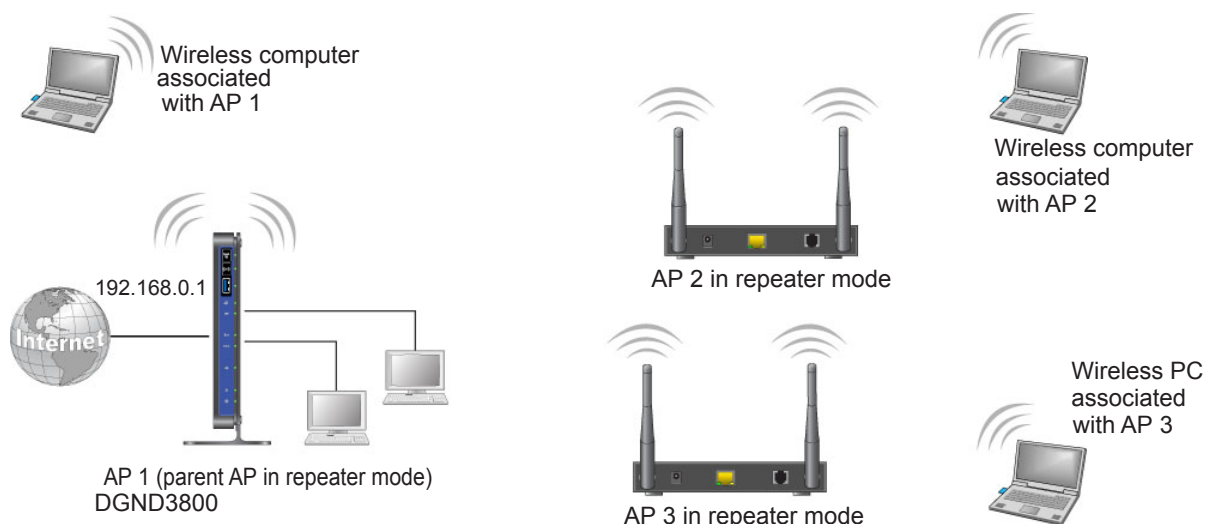

Figure 15. Repeater example

➢ **To set up a repeater with wireless client association:**

In this example, the modem router is the base station, but you can set it up to be the repeater with another AP as the base station if you want.

1. Set up your modem router to be the base station.

   a. In the Wireless Repeating Function screen for your modem router, select the **Enable Wireless Repeating Function** check box.

   b. Select the **Wireless Base Station** radio button.

   c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).

   d. Enter the MAC addresses for AP 2 and AP 3 in the Repeater MAC Address 1 and Repeater MAC Address 2 field.

   e. Click **Apply**.

2. Set up AP 2 and AP 3 to be wireless repeaters.

   a. In the Wireless Repeating Function screen for AP 2 and AP 3, select the **Enable Wireless Repeating Function** check box.

   b. Select the **Wireless Repeater** radio button.

   c. Clear the corresponding **Disable Wireless Client Association** check box (make sure it is not selected).

   d. Enter the MAC addresses for your modem router in the Base Station MAC Address field.

   e. Click **Apply**.

3. Verify the following for all access points:

   • Each access point operates in the same LAN network address range as the LAN devices.

- The access points are on the same LAN. That is, the LAN IP addresses for the access points are in the same network.

- If you are using DHCP, access point devices are set to **Obtain an IP address automatically (DHCP Client)** in the Basic Settings screen.

- Access point devices use the same SSID, channel, authentication mode, and encryption.

Verify connectivity across the LANs. A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.

Remote Management

The Remote Management screen lets you allow a user or users on the Internet to configure, upgrade, and check the status of your modem router.

➢ **To configure remote management:**

1. Select **Advanced > Remote Management** to display this screen:

2. Select the **Turn Remote Management On** check box.

3. Specify the external addresses that can access remote management. For security, restrict access to as few external IP addresses as practical:

- To allow access from a single IP address on the Internet, select **Only This Computer** and enter the IP address that is allowed access.

- To allow access from a range of IP addresses on the Internet, select **IP Address** and enter a beginning and ending IP address to define the allowed range.

- To allow access from any IP address on the Internet, select **Everyone**.

4. Specify the port number to be used for accessing the router interface.

Web browser access usually uses the standard HTTP service port 80. For greater security, you can change it so the remote router interface uses a custom port by entering that number in the field provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** to save your changes.

To access your modem router from the Internet, type your modem router's WAN IP address in your browser's Address field, followed by a colon (:) and the custom port number.

For example, if your external address is 134.177.0.123 at port number 8080, enter the following in your browser:

http://134.177.0.123:8080

The http:// has to be included in the address.

Static Routes

Static routes provide additional routing information to your router. Under normal circumstances, the router has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You have to configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network address is 134.177.0.0.

When you first configured your router, two implicit static routes were created. A default route was created with your ISP as the modem router, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you have to define a static route, telling your router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route setup would look like *Figure 3, Fill in the following fields:*.

In this example:

- The **Destination IP Address** and **IP Subnet Mask** fields specify that this static route applies to all 134.177.x.x addresses.

- The **Gateway IP Address** field specifies that all traffic for these addresses are to be forwarded to the ISDN router at 192.168.0.100.

- The value in the **Metric** field represents the number of routers between your network and the destination. This is a direct connection, so it can be set to the minimum value of 2.

- The **Private** check box is selected only as a precautionary security measure in case RIP is activated.

Static Routes

➢ **To configure static routes:**

1. Select **Advanced > Static Routes** to display the following screen:

2. Click **Add** to open the following screen.

3. Fill in the following fields:

    - **Route Name**. Enter a route name for this static route. This name is for identification purpose only.

    - **Private**. Select this check box if you want to limit access to the LAN only. The static route is not reported in RIP.

    - **Active**. Select this check box to make this route effective.

    - **Destination IP Address**. Enter the IP address of the final destination.

    - **IP Subnet Mask**. Enter the IP subnet mask for this destination. If the destination is a single host, type 255.255.255.255.

    - **Gateway IP Address**. Enter the gateway IP address, which has to be a router on the same LAN segment as the modem router.

    - **Metric**. Enter a number between 2 and 15. This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works.

4. Click **Apply** to save your changes. The Static Routes table is updated to show the new entry.

Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

➢ **To configure Universal Plug and Play:**

1. Select **Advanced > UPnP** to display the following screen:

2. Fill in the settings as follows:

  • **Turn UPnP On**. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is enabled. If UPnP is disabled, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping), of the modem router.

  • **Advertisement Period**. The advertisement period is how often the modem router advertises (broadcasts) its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations might compromise the freshness of the device status but can significantly reduce network traffic.

  • **Advertisement Time To Live**. This is measured in hops (steps) for each UPnP packet sent. Hops are the steps allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value is 4 hops, which works for most home networks. If you notice that some devices are not being updated or reached correctly, you might need to increase this value a little.

  • **UPnP Portmap Table**. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the modem router and which ports (internal

and external) that device has opened. The UPnP Portmap Table also displays what type of port is opened and if that port is still active for each IP address.

3. To save, cancel your changes, or refresh the table:

    *   To save the new settings to the modem router, click **Apply**.

    *   To disregard any unsaved changes, click **Cancel**.

    *   To update the portmap table and to show the active ports that are currently opened by UPnP devices, click **Refresh**.

Traffic Meter

Traffic metering allows you to monitor the volume of Internet traffic passing through your modem router's Internet port. With the Traffic Meter utility, you can set limits for traffic volume, set a monthly limit, and get a live update of traffic usage.

➢ **To monitor traffic on your router:**

1. Select **Advanced > Traffic Meter**.

2. Select the **Enable Traffic Meter** check box.

3. If you would like to record and restrict the volume of Internet traffic, select the **Traffic volume control by** radio button. You can select one of the following options for controlling the traffic volume:

    *   **No Limit**. No restriction is applied when the traffic limit is reached.
    *   **Download only**. The restriction is applied to incoming traffic only.
    *   **Both Directions**. The restriction is applied to both incoming and outgoing traffic.

4. You can limit the amount of data traffic allowed per month:

    *   By specifying how many Mbytes per month are allowed.
    *   By specifying how many hours of traffic are allowed.

5. Set the Traffic Counter to begin at a specific time and date.

6. Set up traffic control to issue a warning message before the monthly limit of Mbytes or hours is reached. You can select one of the following to occur when the limit is attained:

    *   The Internet LED flashes green or amber.
    *   The Internet connection is disconnected and disabled.

7. Set up Internet Traffic Statistics to monitor the data traffic.

8. Click the **Traffic Status** button if you want a live update on Internet traffic status on your router.

9. Click **Apply** to save your settings.

Virtual Private Networking

8

Setting up secure encrypted communications

This chapter describes how to use the virtual private networking (VPN) features of the modem router. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer. The DGND3800B can terminate up to five VPNs.

This chapter is organized as follows:

- *Overview of VPN Configuration*
- *Plan a VPN*
- *VPN Tunnel Configuration*
- *Set Up a Client-to-Gateway VPN Configuration*
- *Set Up a Gateway-to-Gateway VPN Configuration*
- *VPN Tunnel Control*
- *Set Up VPN Tunnels in Special Circumstances*

For additional information, see *Appendix B, VPN Configuration*.

Overview of VPN Configuration

Two common scenarios for VPN tunnels are between a remote computer and a network gateway, and between two or more network gateways. The modem router supports both types. It supports up to five concurrent tunnels.

Client-to-Gateway VPN Tunnels

Client-to-gateway VPN tunnels provide secure access from a remote computer, such as a telecommuter connecting to an office network.
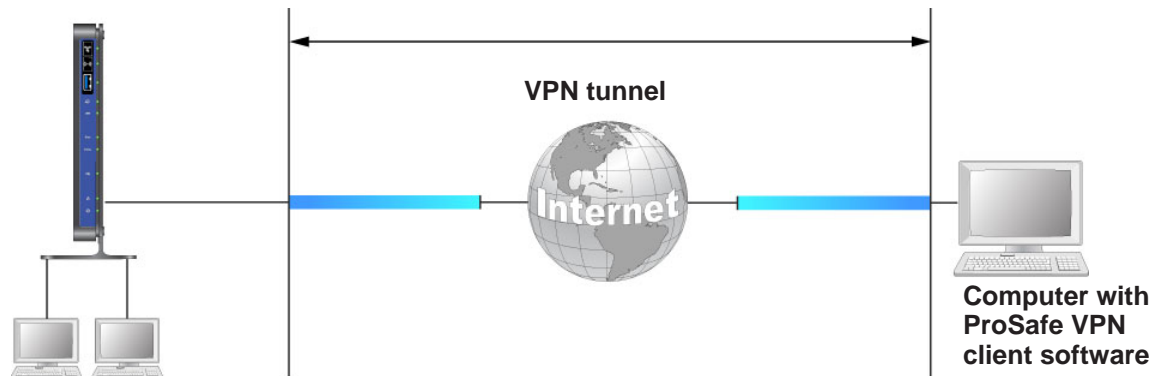
Figure 16. Telecommuter VPN tunnel

A VPN client access allows a remote computer to connect to your network from any location on the Internet. The remote computer is one tunnel endpoint, running the VPN client software. The modem router on your network is the other tunnel endpoint. See *Set Up a Client-to-Gateway VPN Configuration* on page 105 for information about how to set up this configuration.

Gateway-to-Gateway VPN Tunnels

Gateway-to-gateway VPN tunnels provide secure access between networks, such as a branch or home office and a main office.
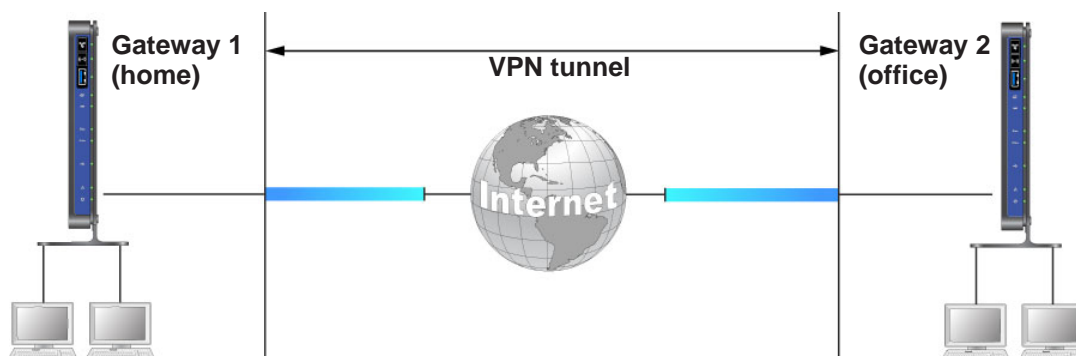
Figure 17. VPN Tunnel between networks

A VPN between two or more NETGEAR VPN-enabled routers is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use gateways on each end of the tunnel to form the VPN tunnel endpoints. See *Set Up a Gateway-to-Gateway VPN Configuration* on page 116 for information about how to set up this configuration.

Plan a VPN

When you set up a VPN, it is helpful to plan the network configuration and record the configuration parameters on a worksheet:

Table 3. VPN tunnel configuration worksheet

Parameter		Value to Be Entered	Field Selection	
Connection Name			N/A	
Pre-Shared Key			N/A	
Secure Association		N/A	Main Mode	Manual Keys
Perfect Forward Secrecy		N/A	Enabled	Disabled
Encryption Protocol		N/A	DES	3DES
Authentication Protocol		N/A	MD5	SHA-1
Diffie-Hellman (DH) Group		N/A	Group 1	Group 2
Key Life in seconds			N/A	
IKE Life Time in seconds			N/A	
VPN Endpoint	**Local IPSecID**	**LAN IP Address**	**Subnet Mask**	**FQDN or Gateway IP (WAN IP Address**

To set up a VPN connection, you have to configure each endpoint with specific identification and connection information describing the other endpoint. You have to configure the outbound VPN settings on one end to match the inbound VPN settings on other end, and vice versa.

This set of configuration information defines a security association (SA) between the two VPN endpoints. When planning your VPN, you should make a few choices first:

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single computer?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single computer?

- Will either endpoint use fully qualified domain names (FQDNs)? FQDNs supplied by Dynamic DNS providers (see *Use a Fully Qualified Domain Name (FQDN)* on page 154) can allow a VPN endpoint with a dynamic IP address to initiate or respond to a tunnel request. Otherwise, the side using a dynamic IP address has to always be the initiator.
- Which method will you use to configure your VPN tunnels?
  - The VPN Wizard using VPNC defaults (see the following table)
  - The typical automated Internet Key Exchange (IKE) setup (see *Use Auto Policy to Configure VPN Tunnels* on page 126)
  - A manual keying setup in which you have to specify each phase of the connection (see *Use Manual Policy to Configure VPN Tunnels* on page 133)

Table 4. Parameters recommended by the VPNC and used in the VPN Wizard

Parameter	Factory Default Setting
Secure Association	Main Mode
Authentication Method	Pre-Shared Key
Encryption Method	3DES
Authentication Protocol	SHA-1
Diffie-Hellman (DH) Group	Group 2 (1024 bit)
Key Life	8 hours
IKE Life Time	1 hour

- What level of IPSec VPN encryption will you use?
  - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
  - **3DES**. Triple DES achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- What level of authentication will you use?
  - **MDS**. 128 bits, faster but less secure.
  - **SHA-1**. 160 bits, slower but more secure.

VPN Tunnel Configuration

There are two tunnel configurations and three ways to configure them:

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
  - See *Set Up a Client-to-Gateway VPN Configuration* on page 105.
  - See *Set Up a Gateway-to-Gateway VPN Configuration* on page 116.

- When the VPN Wizard and its VPNC defaults (see *Table 4* on page 104) are not appropriate for your special circumstances, but you want to automate the Internet Key Exchange (IKE) setup, see *Use Auto Policy to Configure VPN Tunnels* on page 126.

- When the VPN Wizard and its VPNC defaults (see *Table 4* on page 104) are not appropriate for your special circumstances and you have to specify each phase of the connection, see *Use Manual Policy to Configure VPN Tunnels* on page 133. You manually enter all the authentication and key parameters. You have more control over the process; however, the process is more complex, and there are more opportunities for errors or configuration mismatches between your N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B and the corresponding VPN endpoint gateway or client workstation.

Set Up a Client-to-Gateway VPN Configuration

Setting up a VPN between a remote computer running the NETGEAR ProSafe VPN client and a network gateway involves two steps, described in the following sections:

- *Step 1: Configure the Client-to-Gateway VPN Tunnel* on page 105 describes how to use the VPN Wizard to configure the VPN tunnel between the remote computer and network gateway.

- *Step 2: Configure the NETGEAR ProSafe VPN Client* on page 108 shows how to configure the NETGEAR ProSafe VPN client endpoint.

VPN tunnel

IP: 192.168.3.1

22.23.24.25

0.0.0.0

Internet

Computer with ProSafe VPN client software
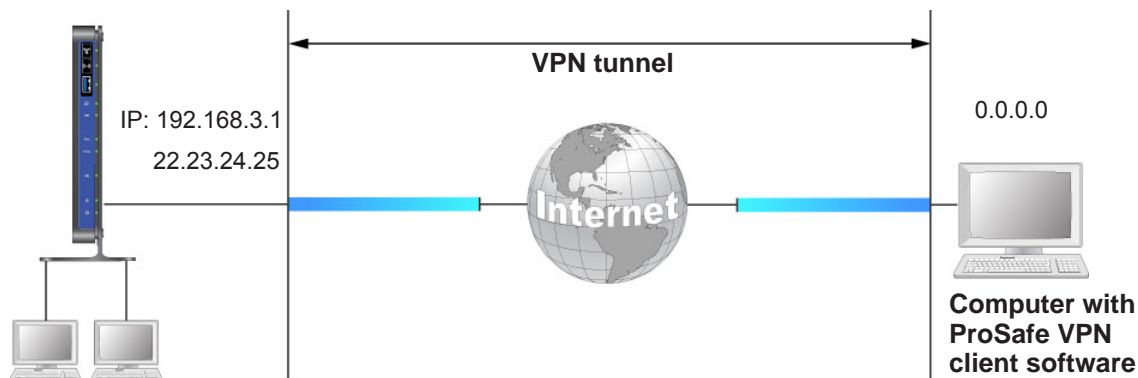
Figure 18. Client-to-gateway VPN tunnel

Step 1: Configure the Client-to-Gateway VPN Tunnel

This section describes using the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in *Table 4* on page 104. If you have special requirements not covered by these VPNC-recommended parameters, see *Set Up VPN Tunnels in Special Circumstances* on page 125 for information about how to set up the VPN tunnel.

The following worksheet identifies the parameters used in this procedure. For a blank worksheet, see *Plan a VPN* on page 103.

Table 5. VPN tunnel configuration worksheet

Parameter	Value to Be Entered	Field Selection		
Connection Name	RoadWarrior	N/A		
Pre-Shared Key	12345678	N/A		
Secure Association	N/A	Main Mode	Manual Keys	
Perfect Forward secrecy	N/A	Enabled	Disabled	
Encryption Protocol	N/A	DES	3DES	
Authentication Protocol	N/A	MD5	SHA-1	
Diffie-Hellman (DH) Group	N/A	Group 1	Group 2	
Key Life in seconds	28800 (8 hours)	N/A		
IKE Life Time in seconds	3600 (1 hour)	N/A		
VPN Endpoint	**Local IPSecID**	**LAN IP Address**	**Subnet Mask**	**FQDN or Gateway IP (WAN IP Address)**
Client	toGateway	N/A	N/A	Dynamic
Gateway	toClient	192.168.3.1	255.255.255.0	22.23.24.25

➢ **To configure a client-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **Advanced > VPN Wizard**.
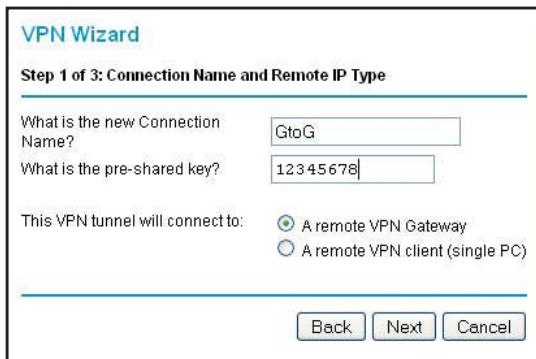
2. Click **Next** to proceed.
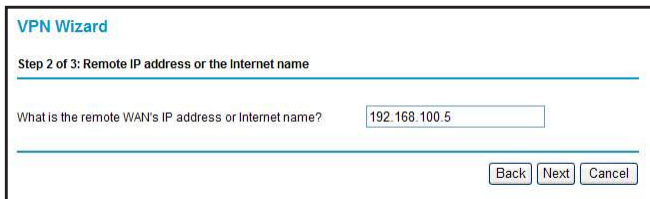
3. Fill in the Connection Name and pre-shared key fields.

The connection name is for convenience and does not affect how the VPN tunnel functions.

4. Select the radio button for the type of target end point, and click **Next**.
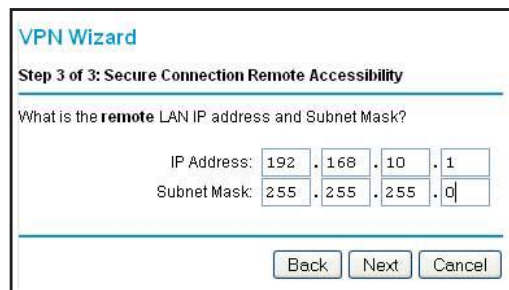
5. Enter the remote IP address, and click **Next**.
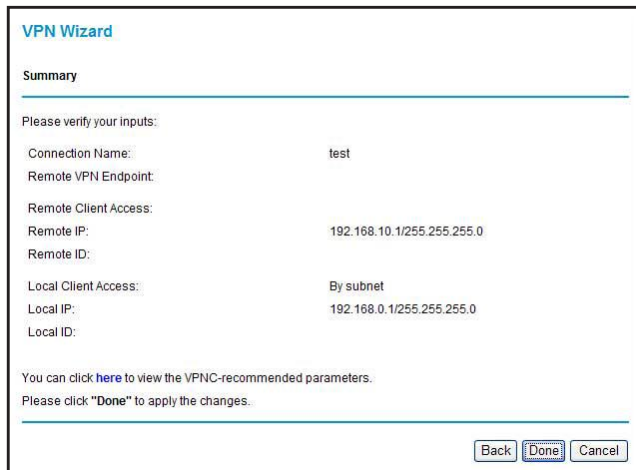
The Summary screen displays:

> **Note:** To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link.

6. Click **Done** on the Summary screen. The VPN Policies screen displays, showing that the new tunnel is enabled:

To view or modify the tunnel settings, select its radio button and click **Edit**.

> **Note:** See *Use Auto Policy to Configure VPN Tunnels* on page 126 for information about how to enable the IKE keep-alive capability on an existing VPN tunnel.

Step 2: Configure the NETGEAR ProSafe VPN Client

This section describes how to configure the NETGEAR ProSafe VPN client on a remote computer. These instructions assume that the computer running the client has a dynamically assigned IP address.

The computer has to have the NETGEAR ProSafe VPN Client program installed, which supports IPSec. Go to the NETGEAR website (*http://www.netgear.com*) for information about how to purchase the NETGEAR ProSafe VPN client.

Note: Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you might be running on your computer. You might need to insert your Windows CD to complete the installation.

➢ **To configure the NETGEAR ProSafe VPN client:**

1. Install the NETGEAR ProSafe VPN client on the remote computer, and then reboot.

   a. Install the IPSec component. You might have the option to install either the VPN adapter or the IPSec component or both. The VPN adapter is not necessary.

      If you do not have a modem or dial-up adapter installed in your computer, you might see the warning message stating, "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.

   b. Reboot the remote computer.

      The ProSafe icon ( ) is in the system tray.

   c. Double-click the ProSafe icon to open the Security Policy Editor.

2. Add a new connection.

   a. Run the NETGEAR ProSafe Security Policy Editor program, and, using *Table 5* on page 106, create a VPN connection.

   b. From the Edit menu of the Security Policy Editor, select **Add**, and then click **Connection**.
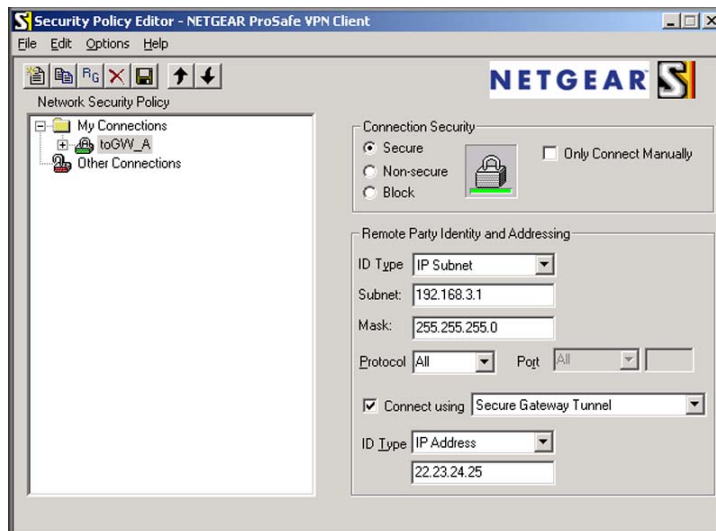
A New Connection listing appears in the list of policies.

c. Rename the new connection so that it matches the Connection Name field in the VPN Settings screen of the modem router on LAN A. Choose connection names that make sense to the people using and administering the VPN.

Note: In this example, the connection name used on the client side of the VPN tunnel is togw_a, and it does not have to match the RoadWarrior connection name used on the gateway side of the VPN tunnel because connection names are irrelevant to how the VPN tunnel functions.

---

d. Enter the following settings:

- **Connection Security**. Select **Secure**.
- **ID Type**. Select **IP Subnet**.
- **Subnet**. In this example, type **192.168.3.1** as the network address of the modem router.
- **Mask**. Enter **255.255.255.0** as the LAN subnet mask of the modem router.
- **Protocol**. Select **All** to allow all traffic through the VPN tunnel.

e. Select the **Connect using Secure Gateway Tunnel** check box.

f. In the **ID Type** drop-down list, select **IP Address**.

g. Enter the public WAN IP address of the modem router in the field directly below the **ID Type** drop-down list. In this example, **22.23.24.25** is used.

The resulting connection settings are shown in the figure that follows.

3. Configure the security policy in the NETGEAR ProSafe VPN Client software:

a. In the Network Security Policy list, expand the new connection by double-clicking its name or clicking the **+** symbol. My Identity and Security Policy subheadings appear below the connection name.

b. Click the **Security Policy** subheading to view the Security Policy settings.
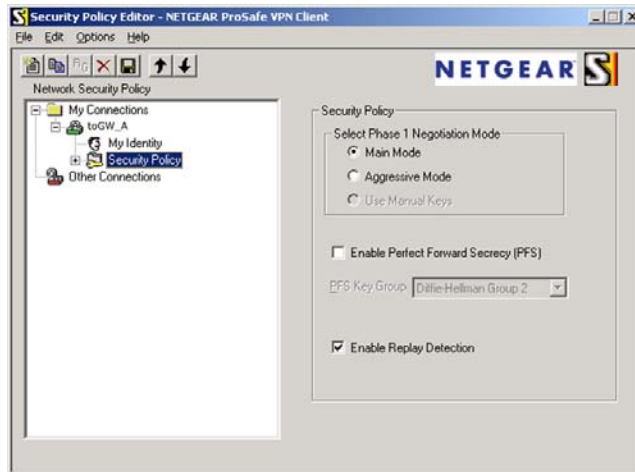
Figure 19. Security Policy settings, Client-to-Gateway A

c. In the Select Phase 1 Negotiation Mode section of the screen, select the **Main Mode** radio button.
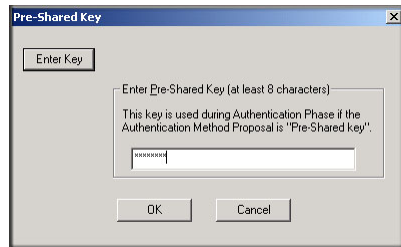
4. Configure the VPN client identity.

In this step, you provide information about the remote VPN client computer. You have to provide the pre-shared key that you configured in the modem router and either a fixed IP address or a fixed virtual IP address of the VPN client computer.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, click **My Identity**.
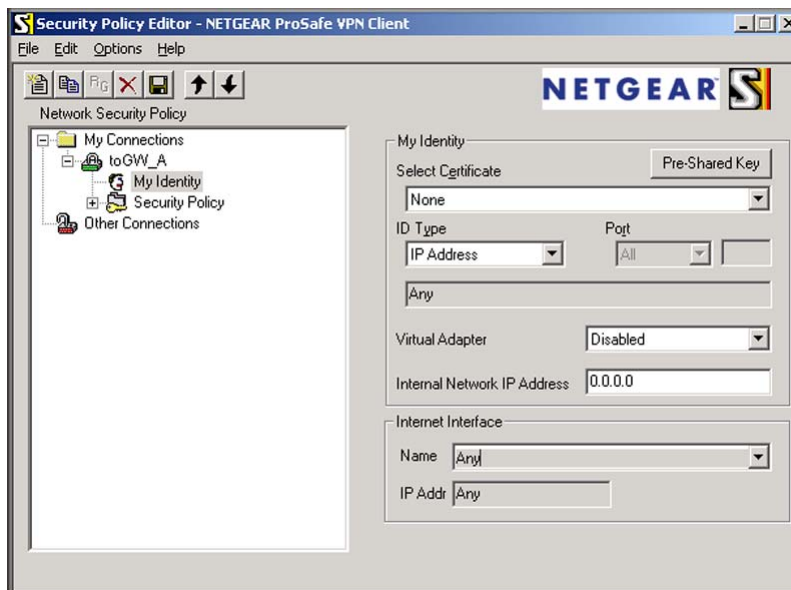
b. In the Select Certifica**te** drop-down list, select **None**.

c. In the ID Type drop-down list, select **IP Address**. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address field. Otherwise, leave this field empty.

d. In the Internet Interface section of the screen, select the adapter that you use to access the Internet. If you have a dial-up Internet account, in the Name list, select **PPP Adapter**. If you have a dedicated cable or ADSL line, select your Ethernet adapter. If you will be switching between adapters or if you have only one adapter, select **Any**.

e. In the My Identity section of the screen, click the **Pre-Shared Key** button. The Pre-Shared Key screen displays:

f. Click **Enter Key**. Enter the modem router pre-shared key, and then click **OK**. In this example, 12345678 is entered, though asterisks are displayed in the field. This field is case-sensitive.

5. Configure the VPN client authentication proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the modem router configuration.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double-clicking its name or clicking the **+** symbol.

b. Expand the Authentication subheading by double-clicking its name or clicking the **+** symbol. Then select **Proposal 1** below Authentication.

c. In the **Authentication Method** drop-down list, select **Pre-Shared key**.

d. In the **Encrypt Alg** drop-down list, select the type of encryption that is configured for the encryption protocol in the modem router, as listed in *Table 3* on page 103. This example uses Triple DES.

    e. In the **Hash Alg** drop-down list, select **SHA-1**.

    f. In the **SA Life** drop-down list, select **Unspecified**.

    g. In the **Key Group** drop-down list, select **Diffie-Hellman Group 2**.

6. Configure the VPN client key exchange proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the modem router configuration.

    a. Expand the Key Exchange subheading by double-clicking its name or clicking the **+** symbol. Then select **Proposal 1** below Key Exchange.

    b. In the **SA Life** drop-down list, select **Unspecified**.

    c. In the **Compression** drop-down list, select **None**.

    d. Select the **Encapsulation Protocol (ESP)** check box.

    e. In the **Encrypt Alg** drop-down list, select the type of encryption that is configured for the encryption protocol in the modem router, as listed in *Table 3* on page 103. This example uses Triple DES.

    f. In the **Hash Alg** drop-down list, select **SHA-1**.

    g. In the **Encapsulation** drop-down list, select **Tunnel**.

    h. Leave the **Authentication Protocol (AH)** check box cleared.

7. Save the VPN client settings.

In the Security Policy Editor window, select **File > Save**.

After you have configured and saved the VPN client information, your computer automatically opens the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

8. Check the VPN connection.

To check the VPN connection, you can initiate a request from the remote computer to the modem router's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports the results of the attempt to connect. Since the

remote computer has a dynamically assigned WAN IP address, it has to initiate the request.

To perform a ping test using our example, start from the remote computer:

a. Establish an Internet connection from the computer.

b. On the Windows taskbar, click the **Start** button, and then select **Run**.

c. Type `ping -t 192.168.3.1`, and then click **OK**.

This causes a continuous ping to be sent to the first modem router. After between several seconds and 2 minutes, the ping response should change from `timed out` to `reply`.

Once the connection is established, you can open a browser on the computer and enter the LAN IP address of the remote gateway. After a short wait, you should see the login screen of the modem router (unless another computer is already logged in to the modem router).

You can view information about the progress and status of the VPN client connection by opening the NETGEAR ProSafe Log Viewer.

To launch this function, click the Windows **Start** button, then select **Programs > NETGEAR ProSafe VPN Client > Log Viewer**. The VPN Status/Log screen for a successful connection is shown in the following figure:
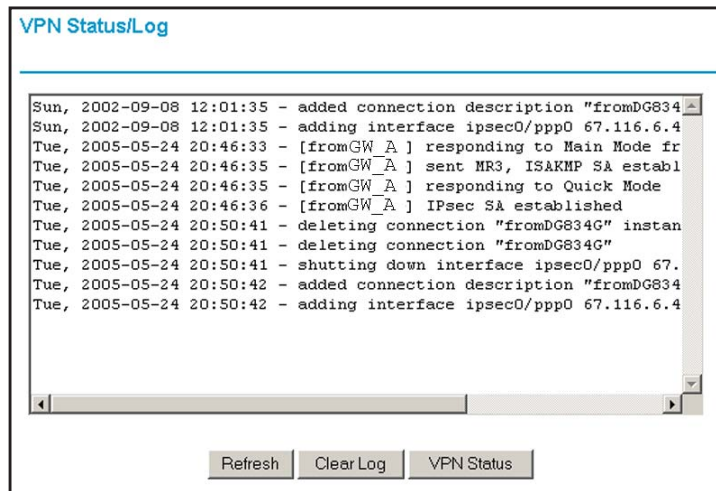
Note: Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

The Connection Monitor screen for this connection is shown in the following figure:
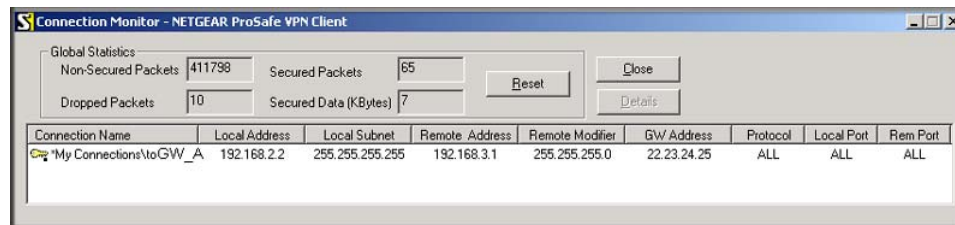
In this example you can see these settings:

- The modem router has a GW address (public IP WAN address) of 22.23.24.25.

- The modem router has a remote address (LAN IP address) of 192.168.3.1.

- The VPN client computer has a local address (dynamically assigned address) of 192.168.2.2.

While the connection is being established, the **Connection Name** field in this screen displays **SA** before the name of the connection. When the connection is successful, the **SA** changes to the yellow key symbol shown in the previous figure.

While your computer is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you have to close the VPN connection to have normal Internet access.

Set Up a Gateway-to-Gateway VPN Configuration

This section describes how to use the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in *Table 4* on page 104. If you have special requirements not covered by these VPNC-recommended parameters, see *Set Up VPN Tunnels in Special Circumstances* on page 125 for information about how to set up the VPN tunnel.
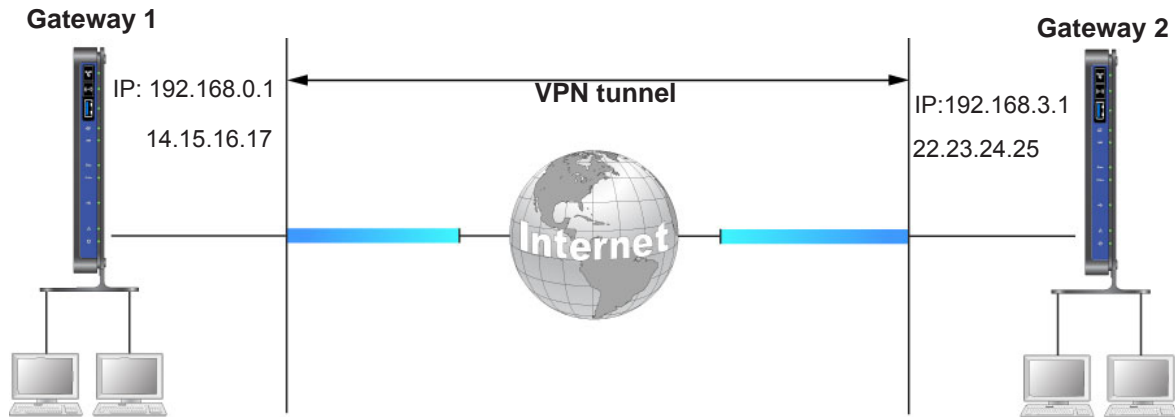
Figure 20. Gateway-to-gateway VPN tunnel

Follow this procedure to configure a gateway-to-gateway VPN tunnel using the VPN Wizard. Set the LAN IPs on each modem router to different subnets and configure each correctly for the Internet. The subsequent examples assume the settings shown in the following table.

Table 6. Gateway-to-gateway VPN tunnel configuration worksheet

Parameter		Value to Enter	Field Selection	
Connection Name		GtoGr	N/A	
Pre-Shared Key		12345678	N/A	
Secure Association		N/A	Main Mode	Manual Keys
Perfect Forward Secrecy		N/A	Enabled	Disabled
Encryption Protocol		N/A	DES	3DES
Authentication Protocol		N/A	MD5	SHA-1
Diffie-Hellman (DH) Group		N/A	Group 1	Group 2
Key Life in seconds		28800 (8 hours)	N/A	
IKE Life Time in seconds		3600 (1 hour)	N/A	
VPN Endpoint	Local IPSecID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address)
Gateway_A	GW_A	192.168.0.1	255.255.255.0	14.15.16.17
Gateway_B	GW_B	192.168.3.1	255.255.255.0	22.23.24.25

Note: The LAN IP address ranges of each VPN endpoint has to be different. The connection fails if both are using the NETGEAR default address range of 192.168.0.x.

➢ **To configure a gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Log in to Gateway A on LAN A. Select **Advanced > VPN Wizard**. Click **Next**, and the Step 1 of 3 screen displays.

2. Fill in the Connection Name and pre-shared key fields. Select the radio button for the type of target endpoint, and click **Next**, and the Step 2 of 3 screen displays.

3. Fill in the IP address or FQDN for the target VPN endpoint WAN connection, and click **Next**. and the Step 3 of 3 screen displays.

4. Fill in the **IP Address** and **Subnet Mask** fields for the target endpoint that can use this tunnel, and click **Next**.

The VPN Wizard Summary screen displays:

To view the VPNC-recommended authentication and encryption settings used by the VPN Wizard, click the **here** link.

5. Click **Done** on the Summary screen.

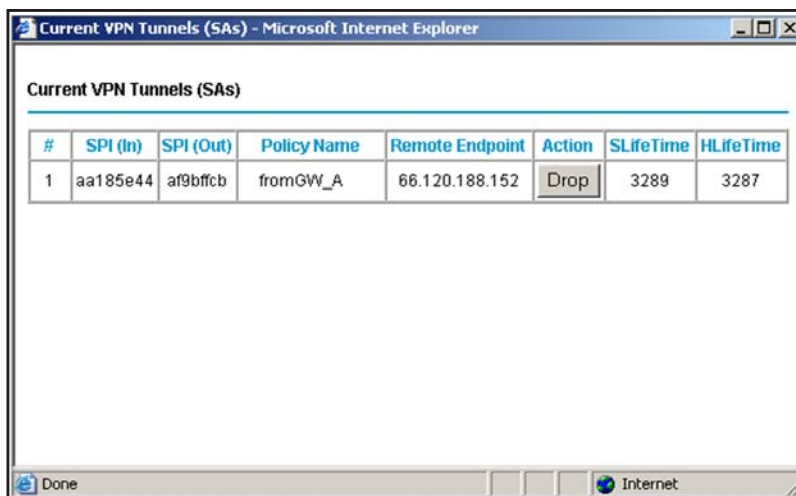The VPN Policies screen displays, showing that the new tunnel is enabled.

Note: See *Use Auto Policy to Configure VPN Tunnels* on page 126 for information about how to enable the IKE keep-alive capability on an existing VPN tunnel.

---

6. Repeat these steps for the gateway on LAN B, and pay special attention to the following network settings:

   - WAN IP of the remote VPN gateway (for example, 14.15.16.17)
   - LAN IP settings of the remote VPN gateway:
     - IP address (for example, 192.168.0.1)
     - Subnet mask (for example, 255.255.255.0)
     - Pre-shared key (for example, 12345678)

7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

> **Note:** The VPN Status screen is only one of three ways to active a VPN tunnel. See *Activate a VPN Tunnel* on page 120 for information about the other ways.

a. Select **Advanced > VPN Status**. The VPN Status/Log screen displays:
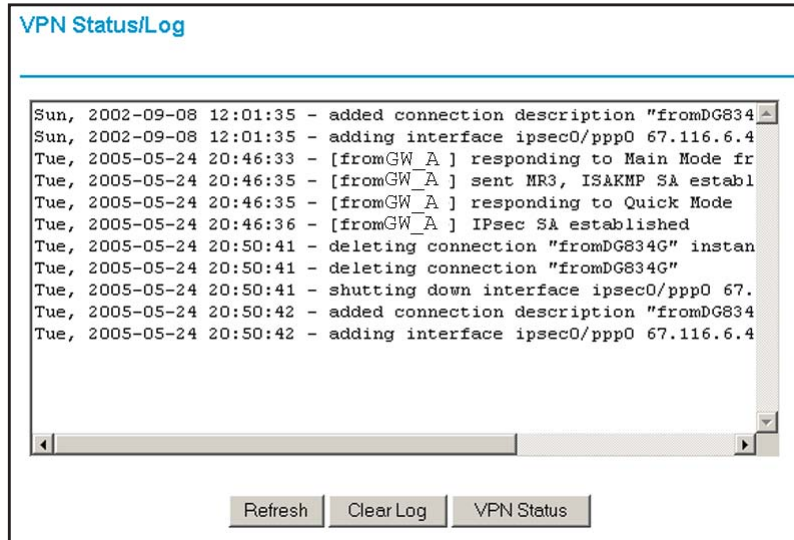
b. Click the **VPN Status** button to display the Current VPN Tunnels (SAs) screen:
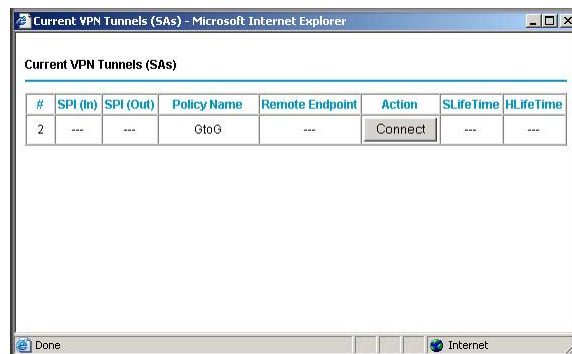
c. Click **Connect** for the VPN tunnel you want to activate. View the VPN Status/Log screen to verify that the tunnel is connected.

VPN Tunnel Control

Activate a VPN Tunnel

There are three ways to activate a VPN tunnel:

- Use the VPN Status screen.
- Ping the remote endpoint.
- Start using the VPN tunnel.

See *Use Auto Policy to Configure VPN Tunnels* on page 126 for information about how to enable the IKE keep-alive capability on an existing VPN tunnel.

➢ **To use the VPN Status screen to activate a VPN tunnel:**

1. Select **Advanced > VPN Status**. The VPN Status/Log screen displays:

   VPN Status/Log

   ```
   Tue, 2004-06-22 22:58:26 - [GtoG]  initiating Main Mode
   Tue, 2004-06-22 22:58:26 - [GtoG]  ISAKMP SA established
   Tue, 2004-06-22 22:58:26 - [GtoG]  sent QI2, IPsec SA established
   Tue, 2004-06-22 22:58:27 - [GtoG]  sent QI2, IPsec SA established
   ```

   Refresh   Clear Log   VPN Status

2. Click **VPN Status** to display the Current VPN Tunnels (SAs) screen:

   Current VPN Tunnels (SAs) - Microsoft Internet Explorer

   Current VPN Tunnels (SAs)

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	aa185e44	af9bffcb	fromGW_A	66.120.188.152	Drop	3289	3287

   Done   Internet
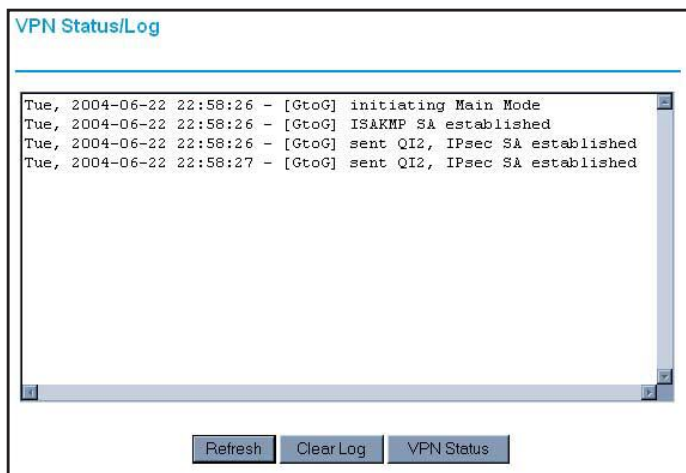
3. Click **Connect** for the VPN tunnel that you want to activate.

Activate the VPN Tunnel by Pinging the Remote Endpoint

This section uses 192.168.3.1 for a sample remote endpoint LAN IP address. To activate the VPN tunnel by pinging the remote endpoint (for example, 192.168.3.1), perform the following steps depending on whether your configuration is client-to-gateway or gateway-to-gateway:

- **Client-to-gateway configuration**. To check the VPN connection, you can initiate a request from the remote computer to the modem router's network by using the Connect option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client reports the results of the attempt to connect. Since the remote computer has a dynamically assigned WAN IP address, it has to initiate the request.

➢ **To perform a ping test using our example, start from the remote computer:**

    a. Establish an Internet connection from the computer.

    b. On the Windows taskbar, click the **Start** button, and then select **Run**.

    c. Type `ping -t 192.168.3.1,` and then click **OK**.

Running a ping test
to the LAN from the computer

    This causes a continuous ping to be sent to the first N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B. Within 2 minutes, the ping response should change from `timed out` to `reply`.

> **Note:** You can use **Ctrl-C** to stop the pinging.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
```

    Once the connection is established, you can open a browser on the computer and enter the LAN IP address of the remote modem router. After a short wait, you should see the login screen of the modem router (unless another computer already has the modem router management interface open).

- **Gateway-to-gateway configuration**. Test the VPN tunnel by pinging the remote network from a computer attached to Gateway A (the modem router).

    a. Open a command prompt (for example, **Start > Run > cmd**).

b. Type **ping 192.168.3.1**.

```
Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=10ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
```

Note: The pings might fail the first time. If they do, then try the pings a second time.

Start Using a VPN Tunnel to Activate It

To use a VPN tunnel, use a web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

Verify the Status of a VPN Tunnel

➢ **To use the VPN Status screen to determine the status of a VPN tunnel:**

1. Select **Advanced > VPN Status** to display the VPN Status/Log screen.

VPN Status/Log

```
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
```

[Refresh]   [Clear Log]   [VPN Status]
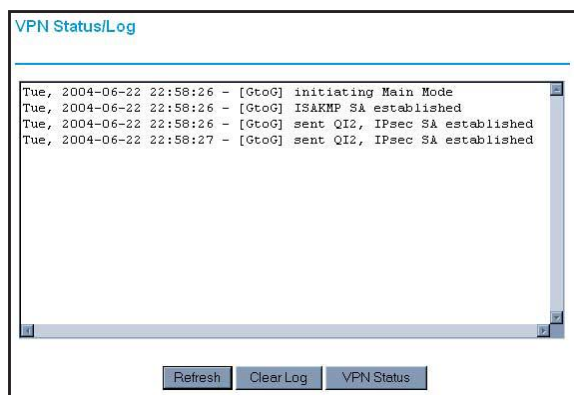
This log shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

- Click **Refresh** to see the most recent entries.
- Click **Clear Log** to delete all log entries.

2. On the VPN Status/Log screen, click **VPN Status** to display the Current VPN Tunnels (SAs) screen.

This table lists the following data for each active VPN tunnel.

- **SPI**. Each SA has a unique SPI (security parameter index) for traffic in each direction. For manual key exchange, the SPI is specified in the policy definition. For automatic key exchange, the SPI is generated by the IKE protocol.

- **Policy Name**. The VPN policy associated with this SA.

- **Remote Endpoint**. The IP address on the remote VPN endpoint.

- **Action**. Either a **Drop** or a **Connect** button.

- **SLifeTime (Secs)**. The remaining soft lifetime for this security association (SA) in seconds. When the soft lifetime becomes 0 (zero), the SA is renegotiated.

- **HLifeTime (Secs)**. The remaining hard lifetime for this SA in seconds. When the hard lifetime becomes 0 (zero), the SA is terminated. (It is reestablished if required.)

Sometimes you need to deactivate a VPN tunnel for testing purposes. You can deactivate a VPN tunnel from two places:

- Policy table on VPN Policies screen
- VPN Status screen

➢ **To deactivate a VPN tunnel:**

1. Select **Advanced > VPN Policies** to display the VPN Policies screen:

2. In the Policy Table, clear the **Enable** check box for the VPN tunnel that you want to deactivate, and then click **Apply**. (To reactivate the tunnel, select the **Enable** check box, and then click **Apply**.)

➢ **To deactivate a VPN tunnel:**

1. Select **Advanced > VPN Policies** to display the VPN Policies screen:

2. Click **VPN Status**. The Current VPN Tunnels (SAs) screen displays:
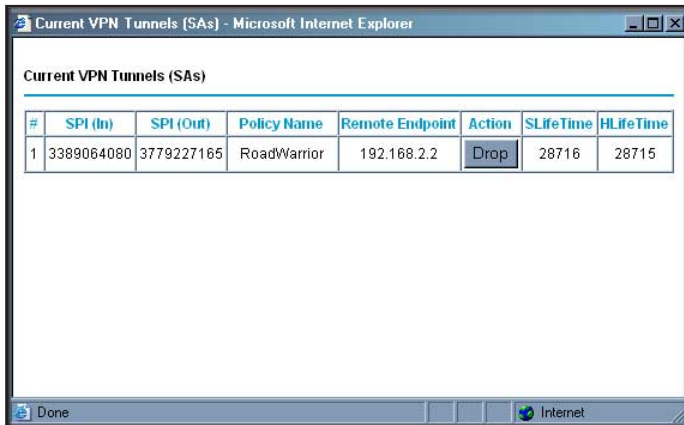
3. Click **Drop** for the VPN tunnel that you want to deactivate.

➢ **To delete a VPN tunnel:**

1. Select **Advanced > VPN Policies** to display the VPN Policies screen.
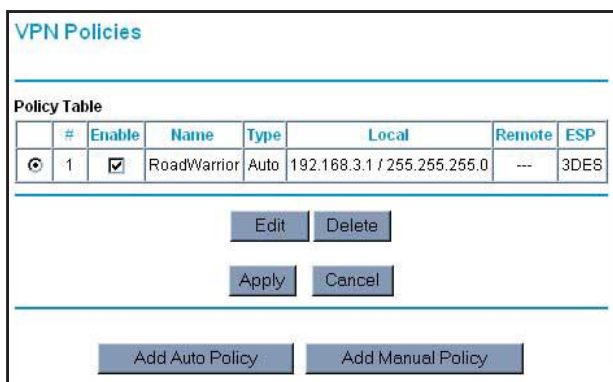
2. In the Policy Table, select the radio button for the VPN tunnel to be deleted, and then click **Delete**.

Set Up VPN Tunnels in Special Circumstances

When the VPN Wizard and its VPNC defaults (see *Table 4* on page 104) are not appropriate for your circumstances, use one of these alternatives:

- **Auto Policy**. For a typical automated Internet Key Exchange (IKE) setup, see *Use Auto Policy to Configure VPN Tunnels* on page 126. Auto Policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys.

- **Manual Policy**. For a manual keying setup in which you have to specify each phase of the connection, see *Use Manual Policy to Configure VPN Tunnels* on page 133. Manual Policy does not use IKE. Rather, you manually enter all the authentication and key parameters. You have more control over the process; however, the process is more complex, and there are more opportunities for errors or configuration mismatches

between your modem router and the corresponding VPN endpoint gateway or client workstation.

Use Auto Policy to Configure VPN Tunnels

You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end has to match to the inbound VPN settings on other end, and vice versa.

For an example of using Auto Policy, see *Example of Using Auto Policy* on page 130.

Configure VPN Network Connection Parameters

All VPN tunnels on the modem router require that you configure several network parameters. This section describes those parameters and how to access them.

The most common configuration scenarios use IKE to manage the authentication and encryption keys. The IKE protocol performs negotiations between the two VPN endpoints to automatically generate and update the required encryption parameters.

Select **Advanced > VPN Policies**, and then click the **Add Auto Policy** button to display the VPN - Auto Policy screen:

The DGND3800B VPN tunnel network connection fields are defined in the following table.

Table 7. VPN - Auto Policy screen settings

Fields and Settings		Description
General	Policy Name	Enter a unique name. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
	Remote VPN Endpoint	• The remote VPN endpoint has to have this VPN's gateway address entered as its remote VPN endpoint. • If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.
	IKE Keep Alive	• If you want to ensure that a connection is kept open, or, if that is not possible, that it is quickly reestablished when disconnected, select this check box. • The ping IP address has to be associated with the remote endpoint. The remote LAN address has to be used. This IP address is pinged periodically to generate traffic for the VPN tunnel. The remote keep-alive IP address has to be covered by the remote LAN IP range and has to correspond to a device that can respond to ping. The range should be made as narrow as possible to meet this objective.
Local LAN The remote VPN endpoint has to have these IP addresses entered as its remote addresses.	Subnet Mask	The network mask.
	Single/Start IP Address	• Enter the IP address for a single address, or the starting address for an address range. A single address setting is used when you want to make a single server on your LAN available to remote users. A range has to be an address range used on your LAN. • **Any**. The remote VPN endpoint can be at any IP address.
	Finish IP Address	For an address range, enter the finish IP address. This has to be an address range used on your LAN.
Remote LAN The remote VPN endpoint has to have these IP addresses entered as its local addresses.	IP Address	**Single Computer - no Subnet**. Select this option if there is no LAN (only a single computer) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a computer running the VPN client at the remote end.
	Single/Start IP Address	• Enter an IP address that is on the remote LAN. You can use this setting when you want to access a server on the remote LAN. • For a range of addresses, enter the starting IP address. This has to be an address range used on the remote LAN. • **Any**. Any outgoing traffic from the computers in the **Local IP** fields triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.
	Finish IP Address	Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.
	Subnet Mask	Enter the network mask.

Table 7. VPN - Auto Policy screen settings (Continued)

Fields and Settings		Description
IKE	Direction	This setting is used when the router determines if the IKE policy matches the current traffic. Select an option. • **Responder only**. Incoming connections are allowed, but outgoing connections are blocked. • **Initiator and Responder**. Both incoming and outgoing connections are allowed.
	Exchange Mode	Ensure that the remote VPN endpoint is set to use **Main Mode**.
	Diffie-Hellman (DH) Group	The Diffie-Hellman algorithm is used when keys are exchanged. The DH Group setting determines the bit size used in the exchange. This value has to match the value used on the remote VPN gateway.
	Local Identity Type	Select an option to match the Remote Identity Type setting on the remote VPN endpoint. • **WAN IP Address**. Your Internet IP address. • **Fully Qualified Domain Name**. Your domain name. • **Fully Qualified User Name**. Your name, email address, or other ID.
	Local Identity Data	Enter the data for the local identity type that you selected. (If WAN IP Address is selected, no input is required.)
	Remote Identity Type	Select the option that matches the **Local Identity Type** setting on the remote VPN endpoint. • **IP Address**. The Internet IP address of the remote VPN endpoint. • **Fully Qualified Domain Name**. The domain name of the remote VPN endpoint. • **Fully Qualified User Name**. The name, email address, or other ID of the remote VPN endpoint.
	Remote Identity Data	Enter the data for the remote identity type that you selected. If IP Address is selected, no input is required.
Parameters	Encryption Algorithm	The encryption algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. DES and 3DES are supported. • **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES. • **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
	Authentication Algorithm	The authentication algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. Auto, MD5, and SHA-1 are supported. Auto negotiates with the remote VPN endpoint and is not available in responder-only mode. • **MD5**. 128 bits, faster but less secure. • **SHA-1**. 160 bits, slower but more secure. This is the default.
	Pre-shared Key	The key has to be entered both here and on the remote VPN gateway.

Table 7. VPN - Auto Policy screen settings (Continued)

Fields and Settings		Description
Parameters (Continued)	SA Life Time	The time interval before the SA (security association) expires. (It is automatically reestablished as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA life-time. This setting applies to both IKE and IPSec SAs.
	Enable IPSec PFS (Perfect Forward Secrecy)	• If this check box is selected, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.) • This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you might have to specify the key group used. For this device, the key group is the same as the DH Group setting in the IKE section.
General	Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
	Remote VPN Endpoint	• The remote VPN endpoint has to have this VPN gateway's address entered as its remote VPN endpoint. • If the remote endpoint has a dynamic IP address, select **Dynamic IP address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.
	IKE Keep Alive	• If you want to ensure that a connection is kept open, or, if that is not possible, that it is quickly reestablished when disconnected, select this check box. • The ping IP address has to be associated with the remote endpoint. The remote LAN address has to be used. This IP address is pinged periodically to generate traffic for the VPN tunnel. The remote keep-alive IP address has to be covered by the remote LAN IP range and has to correspond to a device that can respond to ping. The range should be made as narrow as possible to meet this objective.
Local LAN The remote VPN endpoint has to have these IP addresses entered as its remote addresses.	Subnet Mask	Enter the network mask.
	Single/Start IP Address	• Enter the IP address for a single address, or the starting address for an address range. A single address setting is used when you want to make a single server on your LAN available to remote users. A range has to be an address range used on your LAN. • **Any**. The remote VPN endpoint might be at any IP address.

Example of Using Auto Policy

The following settings are assumed for this example:

Table 8. Gateway-to-gateway VPN tunnel configuration worksheet

Parameter	Value to Be Entered	Field Selection	
Connection Name	GtoG	N/A	
Pre-Shared Key	12345678	N/A	
Secure Association	N/A	Main Mode	Manual Keys
Perfect Forward secrecy	N/A	Enabled	Disabled
Encryption Protocol	N/A	DES	3DES
Authentication Protocol	N/A	MD5	SHA-1
Diffie-Hellman (DH) Group	N/A	Group 1	Group 2
Key Life in seconds	28800 (8 hours)	N/A	
IKE Life Time in seconds	3600 (1 hour)	N/A	

VPN Endpoint	Local IPSecID	LAN IP Address	Subnet Mask	FQDN or Gateway IP (WAN IP Address
Gateway_A	GW_A	192.168.0.1	255.255.255.0	14.15.16.17
Gateway_B	GW_B	192.168.3.1	255.255.255.0	22.23.24.25

➢ **To use this auto policy example:**

1. Set the LAN IPs on each router to different subnets and configure each correctly for the Internet.

2. Select **Advanced > VPN Policies** and click the **Add Auto Policy** button. The VPN - Auto Policy screen displays:

3. Enter these policy settings:

Auto Policy Field		Description
General	Policy Name	GtoG
	Remote VPN Endpoint Address Type	Fixed
	Remote VPN Endpoint Address Data	22.23.24.25
Local LAN		Use the default settings.
Remote LAN	IP Address	Select **Subnet address** from the drop-down list.
	Start IP Address	192.168.3.1
	Subnet Mask	255.255.255.0

Auto Policy Field		Description
IKE	Direction	Initiator and Responder
	Exchange Mode	Main Mode
	Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
	Local Identity Type	Use the default setting.
	Remote Identity Type	Use the default setting.
Parameters	Encryption Algorithm	3DES
	Authentication Algorithm	MD5
	Pre-shared Key	12345678

4. Click **Apply**. The VPN Policies screen displays:

5. Repeat these steps for the N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B on LAN B. Pay special attention to the following network settings:
   - General, Remote Address Data (for example, 14.15.16.17)
   - Remote LAN, Start IP Address
     - IP Address (for example, 192.168.0.1)
     - Subnet Mask (for example, 255.255.255.0)
     - Pre-shared Key (for example, 12345678)

6. Use the VPN Status screen to activate the VPN tunnel:

Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See *Activate a VPN Tunnel* on page 120 for information about the other ways.

a. Select **Advanced > VPN Status** to display the VPN Status/Log screen. Then click **VPN Status** to display the Current VPN Tunnels (SAs) screen:
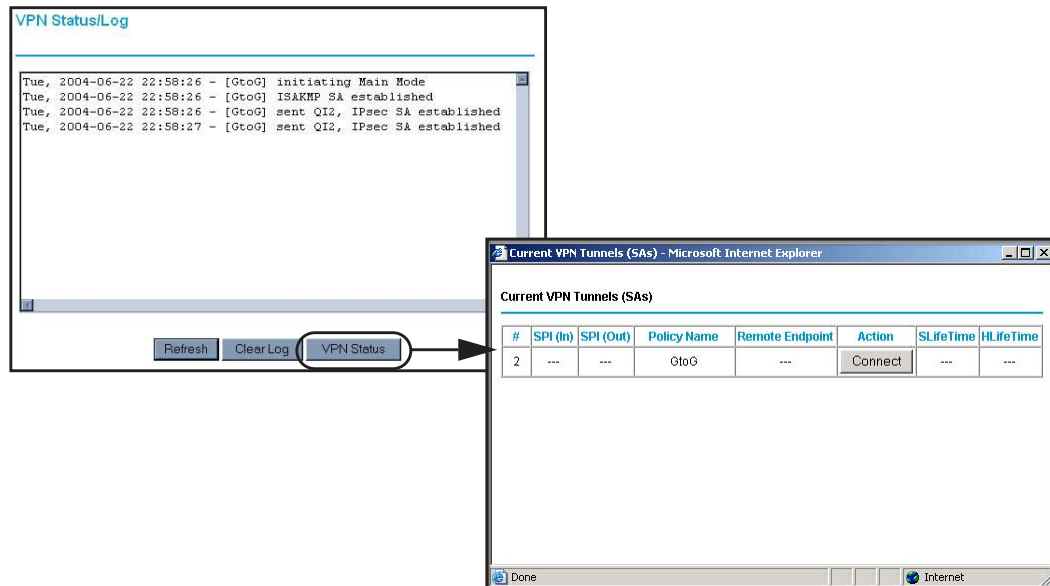
b. Click **Connect** for the VPN tunnel that you want to activate. Review the VPN Status/Log screen (*Figure a* on page 119) to verify that the tunnel is connected.

Use Manual Policy to Configure VPN Tunnels

As an alternative to IKE, you can use manual keying, in which you have to specify each phase of the connection. A manual VPN policy requires all settings for the VPN tunnel to be manually input at each end (both VPN endpoints).

Select **Advanced > VPN Policies**, and then click the **Add Manual Policy** radio button to display the VPN - Manual Policy screen:

The following table explains the fields in the VPN - Manual Policy screen.

Table 9. VPN Manual Policy fields and settings

Fields and Settings		Description
General The modem router VPN tunnel network connection fields.	Policy Name	Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
	Remote VPN Endpoint	• The remote VPN endpoint has to have this VPN's gateway address entered as its remote VPN endpoint. • If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.

Table 9. VPN Manual Policy fields and settings (Continued)

Fields and Settings		Description
Local LAN IP Address The remote VPN endpoint has to have these IP addresses entered as its remote addresses.	Subnet Mask	Enter the network mask.
	Single computer - no Subnet	Select this option if there is no LAN (only a single computer) at the remote endpoint. If this option is selected, no additional data is required.
	Single/Start IP Address	• The IP address for a single address, or the starting address for an address range used on the LAN. If you want to make a single server on your LAN available to remote users, use a single address settings. • **Any**. The remote VPN endpoint can be at any IP address.
	Finish IP Address	For an address range, enter the finish IP address. This has to be an address range used on your LAN.
	Subnet Mask	Enter the network mask.
Remote LAN IP Address The remote VPN endpoint has to have these IP addresses entered as its local addresses.	IP Address	**Single computer - no Subnet**. Select this option if there is no LAN (only a single computer) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a computer running the VPN client at the remote end.
	Single/Start IP Address	• Enter an IP address on the remote LAN. You can use this setting to access a server. • For a range of addresses, enter the starting IP address. This has to be an address range used on the remote LAN. • **Any**. Any outgoing traffic from specified **Local IP** computers triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.
	Finish IP Address	Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.
	Subnet Mask	Enter the network mask.
ESP Configuration ESP (encapsulating security payload) provides security for the payload (data) sent through the VPN tunnel.	SPI	Enter the required security policy indexes (SPIs). Each policy has to have unique SPIs. These settings have to match the remote VPN endpoint. The **in** setting here has to match the **out** setting on the remote VPN endpoint, and the **out** setting here has to match the **in** setting on the remote VPN endpoint.
	Encryption	Select an encryption algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters, and for DES, the keys should be 8 ASCII characters. • **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES. • **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
	Authentication	Select an authentication method.

Troubleshooting 9

Diagnosing and solving problems

This chapter provides information to help you diagnose and solve problems you might have with your modem router. If you do not find the solution here, check the NETGEAR support site at *http://support.netgear.com* for product and contact information.

This chapter contains the following sections:

- *Troubleshooting with the LEDs*
- *No ISP Connection*
- *TCP/IP Network Not Responding*
- *Cannot Log In*
- *Changes Not Saved*
- *Firmware Needs to Be Reloaded*
- *Incorrect Date or Time*

Troubleshooting with the LEDs

When you turn the power on, the Power, LAN, Wireless, DSL, and Internet LEDs should light as described here. If they do not, refer to the sections that follow for help.

1. When power is first applied, the Power LED lights.

2. After approximately 10 seconds, other LEDs light as follows:

   a. The LAN ports LED lights when any local port is connected.

   b. The 2.4 GHz and 5 GHz Wireless LEDs light.

   c. The DSL LED lights when there is a link through the ADSL phone lines.

   d. The Internet LED lights to indicate a connection to the ISP.
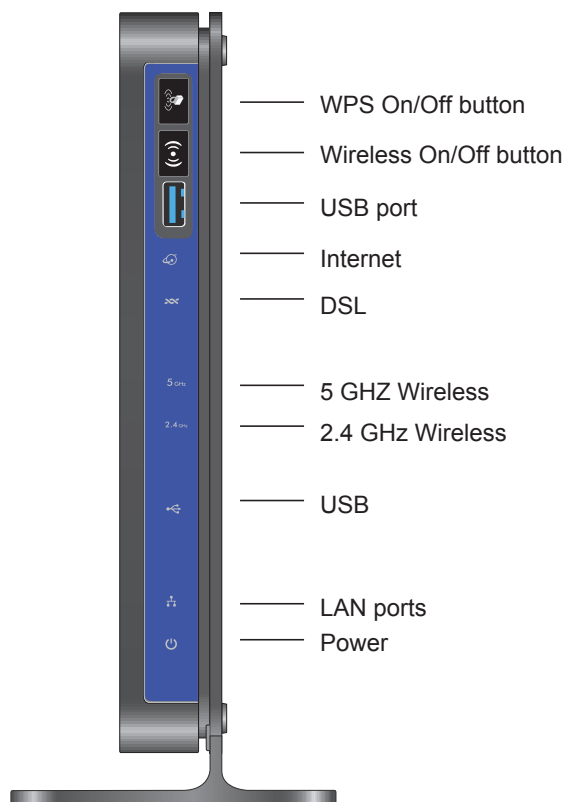
Figure 21. Front panel LEDs

Power LED Is Off

If the Power and other LEDs are off when your router is turned on:

- Check that the power cord is correctly connected to your router and the power supply adapter is correctly connected to a functioning power outlet.

- Check that you are using the 12V DC power adapter supplied by NETGEAR for this product.

If the error persists, you could have a hardware problem and should contact NETGEAR technical support.

Power LED Is Red

When the router is turned on, it performs a power-on self-test. If the Power LED turns red after a few seconds or at any other time during normal operation, there is a fault within the router.

If the Power LED turns red to indicate a router fault, turn the power off and on to see if the modem router recovers. If the power LED is still red 1 minute after power-up:

- Turn the power off and on one more time to see if the modem router recovers.

- Clear the router's configuration to factory defaults as explained in *Factory Settings* on page 147. This sets the router's IP address to 192.168.0.1.

If the error persists, you could have a hardware problem and should contact NETGEAR technical support.

LAN LED Is Off

If the LAN LED does not light when the Ethernet connection is made, check the following:

- The Ethernet cable connections are secure at the modem router and at the hub or workstation.

- The power is turned on to the connected hub or workstation.

Wireless LEDs Are Off

If the 2.4 GHz and 5 GHz Wireless LEDs do not light, the radios might be turned off. Press the **Wireless On/Off** button on the front panel to turn the radios back on.

DSL or Internet LED Is Off

If the DSL or Internet LED does not light, check to make sure that you are using the correct cable. When connecting the ADSL or Ethernet WAN port, use the cables that were supplied with the modem router. If the DSL or Internet LED is still off, this could mean that there is no ADSL or fiber/cable modem service or the cable connected to the ADSL or Ethernet WAN port is bad.

See also *DSL LED Is Off* on page 139.

No ISP Connection

If your router cannot access the Internet, first check the ADSL connection, and then check the WAN TCP/IP connections. See *Figure 21, Front panel LEDs* on page 137 for the location of the LEDs.

ADSL Link

First determine whether you have an ADSL link with the service provider. The state of this connection is indicated by the DSL LED.

DSL LED Is Green or Blinking Green

You have a good ADSL connection. The service provider has connected your line correctly, and your wiring is correct.

DSL LED Is Blinking Amber

Your modem router is attempting to make an ADSL connection with the service provider. The LED should turn green within several minutes.

If the DSL LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone as described in *ADSL Microfilters* on page 13. If you connect the microfilters correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, there might be a problem with your wiring. If the telephone company has tested the ADSL signal at your network interface device (NID), you might have poor-quality wiring in your house.

DSL LED Is Off

First disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time and use a microfilter on each telephone. If the microfilters are connected correctly, you should be able to connect all your telephones.

If disconnecting telephones does not result in a green DSL LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It could be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

Internet LED Is Red

If the Internet LED is red, the device could not connect to the Internet. Verify the following:

- Check that your login credentials are correct. See *Log In to the N600 Modem Router* on page 18 for more information.
- Check that the information you entered on the Basic Settings screen is correct. See *Manual Setup (Basic Settings)* on page 22.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the ADSL settings screen are correct.
- Find out if the ISP is having a problem. If it is, wait until that problem is cleared up and try again.

Cannot Obtain an Internet IP Address

If your modem router cannot access the Internet, and your Internet LED is green or blinking green, check whether the modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem router has to request an IP address from the ISP.

➢ **You can determine whether the request was successful as follows:**

1. Access the router menus at *http://192.168.0.1* and log in.
2. Under Maintenance, select **Router Status** and check that an IP address shows for the WAN port. If 0.0.0.0 shows, your modem router has not obtained an IP address from your ISP.

If your router cannot obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrect. See *Debug PPPoE or PPPoA* on page 141.
- Your ISP might check for your computer's host name. Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard. See *Setup Wizard* on page 21 for more information.
- Your ISP allows only one Ethernet MAC address to connect to the Internet, and might check for your computer's MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device and ask them to use the router's MAC address.
  - Configure your router to spoof your computer's MAC address through the Basic Settings screen. See *Manual Setup (Basic Settings)* on page 22.

Debug PPPoE or PPPoA

➢ **Debug the PPPoE or PPPoA connection as follows:**

1. Access the router menus at *http://192.168.0.1* and log in.

2. Under Maintenance, select **Router Status**.

3. Click the **Connection Status** button.

4. If all of the steps indicate OK, your PPPoE or PPPoA connection is working.

5. If any of the steps indicate Failed, you can attempt to reconnect by clicking **Connect**.

   The modem router continues to attempt to connect indefinitely. If you do not connect after several minutes, check that the service name, user name, and password you are using are correct. Also check with your ISP to be sure that there is no problem with their service.

> **Note:** Unless you connect manually, the modem router does not authenticate with PPPoE or PPPoA until data is transmitted to the network.

Cannot Load an Internet Web Page

If your modem router can obtain an IP address, but your browser cannot load any Internet web pages:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address during the modem router's configuration, reboot your computer, and verify the DNS address. Alternately, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the modem router configured as its TCP/IP modem router.

  If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address.

TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your Modem Router

You can ping the router from your computer to verify that the LAN path to your router is set up correctly.

➢ **To ping the router from a Computer running Windows 95 or later:**

1. From the Windows task bar, click the **Start** button, and select **Run**.

2. In the field provided, type **ping** followed by the IP address of the router, as in this example:

   ping 192.168.0.1

3. Click **OK**.

   You should see a message like this one:

   `Pinging <IP address> with 32 bytes of data`

   If the path is working, you see this message:

   `Reply from < IP address >: bytes=32 time=NN ms TTL=xxx`

   If the path is not working, you see this message:

   `Request timed out`

   If the path is not functioning correctly, you could have one of the following problems:

   • Wrong physical connections

     - Make sure that the LAN port LED is on. If the LED is off, follow the instructions in *LAN LED Is Off* on page 138.

     - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and router.

   • Wrong network configuration

     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.

     - Verify that the IP address for your router and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your computer to a remote device. In the Windows Run screen, type:

ping -n 10 IP address

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as described in *Test the LAN Path to Your Modem Router* on page 142 display. If you do not receive replies:

- Check that your computer has the IP address of your router listed as the default modem router. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default modem router.

- Check that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.

- Check that your cable or ADSL modem is connected and functioning.

- If your ISP assigned a host name to your computer, enter that host name as the account name in the Basic Settings screen.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single computer connected to that modem. In this case, configure your router to clone or spoof the MAC address from the authorized computer.

Cannot Log In

If you cannot log in to the modem router from a computer on your local network, check the following:

- The router is plugged in and it is on.

- You are using the correct login information. The login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

- If you cannot connect wirelessly, try an Ethernet connection and view the router wireless settings and set up your wireless computer with corresponding wireless settings.

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the router. The LAN LED for the port you are using on the router should light up to show your connection.

- Your computer's IP address is on the same subnet as the router. If you are using the recommended addressing scheme, your computer's address should be in the range 192.168.0.2 to 192.168.0.254.

- If the computer IP address is 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address when the computer cannot reach a DHCP server. The

autogenerated addresses are in the range 169.254.x.x. If your IP address is in this range, check the connection from the computer to the router and reboot your computer.

- If your router's IP address was changed and you do not know the current IP address, clear the router's configuration to factory defaults as explained in *Factory Settings* on page 147. This sets the router's IP address to 192.168.0.1.

- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.

- Try closing the browser and relaunching it.

Changes Not Saved

If the router does not save the changes you make in the router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.

- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser's cache.

Firmware Needs to Be Reloaded

When you attempt to connect to the Internet, the browser might display a message similar to the following one telling you that you need to reload the router's firmware. This means a problem has been detected with the router's firmware.

Your Netgear DSL Gateway has detected that its firmware needs to be reloaded.

To reload firmware, please follow these steps:
1. Obtain the firmware to load (from the firmware loaded on your PC during setup with the Setup Wizard CD (default), from the Setup CD, or from the Netgear support site) and place it in a folder on your PC.
2. Browse to the firmware or enter the path in the box below.
3. Click on Upgrade.
4. The upgrade process will take about 5 minutes, wait for the Progress Bar to complete.
5. The Router Management Interface log-in prompt will then appear so you can log in to check the status.

Software file name : [   ] [Browse...] [Upgrade]

Please note: If you used the Setup CD, the PC that you used should have a firmware load at C:\Netgear.

Figure 22. Reload firmware

➢ **To reload the firmware:**

1. If you already have the firmware file on your computer, go directly to step 2. If you do not have the firmware file on your computer, obtain the firmware from the NETGEAR support site at *http://www.netgear.com/support* through another working Internet connection.

2. Click **Browse**.

3. Navigate to the firmware file.

4. Click **Upgrade**. A progress bar displays. The reload takes about 5 minutes to complete. When the firmware recovery is complete, the login screen displays so you can log in.

Incorrect Date or Time

Select **Security > Schedule** to display the current date and time. The modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

*   Date shown is January 1, 2000. This means the router has not yet successfully reached a network time server. Check that your Internet access is configured correctly. If you have just completed configuring the router, wait at least 5 minutes, and check the date and time again.

*   Time is off by one hour. The router does not automatically sense daylight savings time. In the Schedule screen, select the **Adjust for Daylight Savings Time** check box.

Supplemental Information A

This appendix includes the factory default settings and technical specifications for the N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B, and instructions for wall-mounting the unit.

This appendix contains the following sections:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the modem router to its factory settings. On the bottom of the modem router, use the end of a paper clip or some other similar object to press and hold the **Restore Factory Settings** button ⭘ for at least 7 seconds. The modem router resets and returns to the factory settings. Your device returns to the factory configuration settings shown in the following table.

Table 10. Factory settings description

Feature	Default Behavior
Router Login	
User Login URL	http://www.routerlogin.net *or* http://www.routerlogin.com
User Name (case-sensitive)	admin
Login Password (case-sensitive)	password
Internet Connection	
WAN MAC Address	Use default address
WAN MTU Size	1492
Port Speed	AutoSense
Local Network (LAN)	
Lan IP	192.168.0.1
Subnet Mask	255.255.255.0
RIP Direction	None
RIP Version	Disabled
RIP Authentication	None
DHCP Server	Enabled
DHCP Starting IP Address	192.168.0.2
DHCP Ending IP Address	192.168.0.254
DMZ	Disabled
Time Zone	GMT
Time Zone Adjusted for Daylight Saving Time	Disabled
SNMP	Disabled

Table 10. Factory settings description (Continued)

Feature		Default Behavior
Firewall		
	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless		
	Wireless Communication	Enabled
	Wi-Fi Network Name (SSID)	Can be found on the label on the bottom of the unit.
	Wireless security	Can be found on the label on the bottom of the unit.
	Broadcast SSID	Enabled
	Transmission Speed	Auto[1]
	Country/Region	United States (in North America; otherwise, varies by region)
	RF Channel	Auto
	Operating Mode	Up to 145 Mbps
	Data Rate	Best
	Output Power	Full
	Access Point	Enabled
	Authentication Type	Pre-Shared Key
	Wireless Card Access List	All wireless stations allowed

1. *Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.*

Technical Specifications

Table 11. Technical specifications description

Feature	Specification
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
Power adapter	North America: 120V, 60 Hz, input Europe: 230V, 50 Hz, input All regions output: 12V AC @ 2.5A output:
Dimensions	6.80 in. x 5.03 in. x 1.28 in. (172.7 mm x 127.7 mm x 32.5 mm)
Weight	0.61 lbs (0.275 kg)
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	10% to 90% relative humidity, noncondensing
Storage temperature	–20° to 70° C (-4º to 158º F)
Storage humidity	5 to 95% relative humidity, noncondensing
Meets requirements of	FCC Part 15 Class B; VCCI Class B; EN 55 022 (CISPR 22), Class B
LAN	10BASE-T or 100BASE-Tx, RJ-45 (Gigabit Ethernet)
WAN	ADSL, Dual RJ-11, pins 2 and 3 T1.413, G.DMT RJ-45 WAN port (Gigabit Ethernet)

VPN Configuration

Case study on how to set up a VPN

B

The DGND3800B can terminate up to five VPNs. This appendix is a case study on how to configure a secure IPSec VPN tunnel from your modem router to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

The following topics are discussed:

- *Configuration Profile*
- *Modem Router with FQDN to Gateway B*
- *Configuration Summary (Telecommuter Example)*
- *Set Up Client-to-Gateway VPN (Telecommuter Example)*
- *Monitoring the VPN Tunnel (Telecommuter Example)*

Configuration Profile

The configuration in this appendix follows the addressing and configuration mechanics defined by the VPN Consortium. Gather necessary information before you begin configuration. Verify that the firmware is up to date, and that you have all the addresses and parameters to be set on both sides. Check that there are no firewall restrictions.

Table 12. Wireless modem router to Gateway B profile summary

VPN Consortium Scenario	Scenario 1 (Identity Using Preshared Secrets)
Type of VPN	LAN-to-LAN or gateway-to-gateway (not client-to-gateway)
Security scheme:	IKE with pre-shared secret/key (not certificate based)
IP addressing:	
Gateway A	Static IP address
Gateway B	Static IP address

10.506.0/24   172.23.9.0/24

Gateway A
(DGND3800)

Gateway B

Internet

LAN IP
10.5.6.1

WAN IP
14.15.16.17

WAN IP
22.23.24.25

LAN IP
172.23.9.1
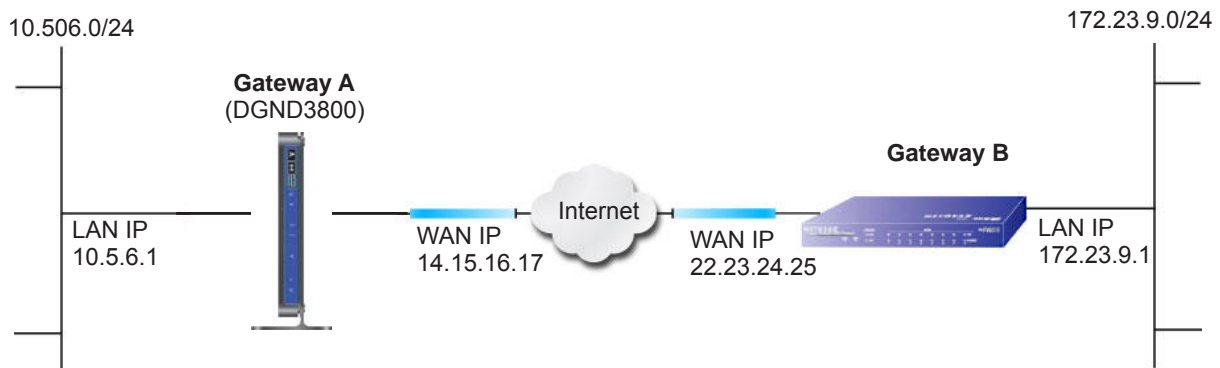
Figure 23. VPNC example, network interface addressing

Step-by-Step Configuration

➢ **To configure a VPN tunnel:**

1. Use the VPN Wizard to configure Gateway A (DGND3800B) for a gateway-to-gateway tunnel (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 116), being certain to use appropriate network addresses for the environment.

   The LAN addresses used in this example are as follows:

Unit	WAN IP	LAN IP	LAN Subnet Mask
DGND3800B	14.15.16.17	10.5.6.1	255.255.255.0
FVL328	22.13.24.25	172.23.9.1	255.255.255.0

   a. For the connection name, enter **toGW_B**.

   b. For the remote WAN's IP address, enter **22.23.24.25**.

   c. Enter the following:

     • IP Address. **172.23.9.1**

     • Subnet Mask. **255.255.255.0**

   d. In the Summary screen, click **Done**.

2. Use the VPN Wizard to configure the Gateway B for a gateway-to-gateway tunnel (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 116), being certain to use appropriate network addresses for the environment.

   a. For the connection name, enter **toGW_A**.

   b. For the remote WAN's IP address, enter **14.15.16.17**.

   c. Enter the following:

     • IP Address. **10.5.6.1**

     • Subnet Mask. **255.255.255.0**

   d. In the Summary screen, click **Done**.

3. On the Gateway B router menu, under VPN, select **IKE Policies**, and click the **Edit** button to display the IKE Policy Configuration screen:

IKE Policy Configuration

General
Policy Name — toGW_A
Direction/Type — Both Directions
Exchange Mode — Main Mode

Local
Local Identity Type — WAN IP Address
Local Identity Data — 22.23.24.25

Remote
Remote Identity Type — Remote WAN IP
Remote Identity Data — 14.15.16.17

IKE SA Parameters
Encryption Algorithm — 3DES
Authentication Algorithm — SHA-1
Authentication Method — ● Pre-shared Key
****
○ RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group — Group 2 (1024 Bit)
SA Life Time — 28800 (secs)

Back   Apply   Cancel

4. On Gateway B router menu, under VPN, select **VPN Policies**, and click the **Edit** button to display the VPN - Auto Policy screen:

VPN - Auto Policy

General
Policy Name — toGW_A
IKE policy — toGW_A
☐ IKE Keep Alive — Ping IP Address: 0 . 0 . 0 . 0
Remote VPN Endpoint — Address Type: IP Address
Address Data: 14.15.16.17
SA Life Time — 86400 (Seconds)
0 (Kybtes)
☐ IPSec PFS — PFS Key Group: Group 1 (768 Bit)
☑ NetBIOS Enable

Traffic Selector
Local IP — Subnet address
Start IP address: 192 . 168 . 2 . 0
Finish IP address: 172 . 23 . 9 . 1
Subnet Mask: 255 . 255 . 255 . 0
Remote IP — Subnet address
Start IP address: 192 . 168 . 0 . 1
Finish IP address: 0 . 10 . 5 . 6
Subnet Mask: 255 . 255 . 255 . 0

AH Configuration
☐ Enable Authentication — Authentication Algorithm: MD5

ESP Configuration
☑ Enable Encryption — Encryption Algorithm: 3DES
☑ Enable Authentication — Authentication Algorithm: SHA-1
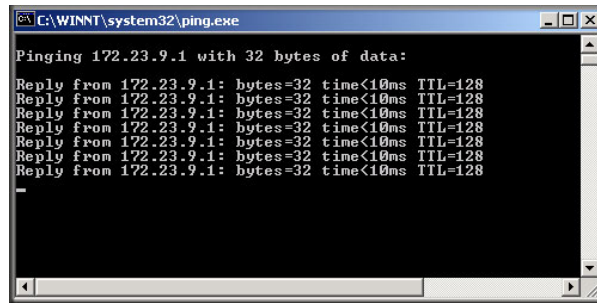
Back   Apply   Cancel

5. Test the VPN tunnel by pinging the remote network from a computer attached to Gateway A (modem router).

   a. Open the command prompt (select **Start > Run > cmd**).

b. Type `ping 172.23.9`.

```
C:\WINNT\system32\ping.exe                                    _ □ ×

Pinging 172.23.9.1 with 32 bytes of data:

Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
```

If the pings fail the first time, try the pings a second time.

Modem Router with FQDN to Gateway B

This section is a case study on how to configure a VPN tunnel from your modem router to a gateway using a fully qualified domain name (FQDN) to resolve the public address of one or both routers. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

Configuration Profile

The configuration in this section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather the necessary information before you begin configuration. Verify that the firmware is up to date, and that you have all the addresses and parameters to be set on both sides. Check that there are no firewall restrictions.

10.506.0/24   172.23.9.0/24

Gateway A
(DGND3700)

Gateway B

Internet

LAN IP
10.5.6.1

WAN IP
example.org
(FQDN)

WAN IP
example2.org
(FQDN)

LAN IP
172.23.9.1
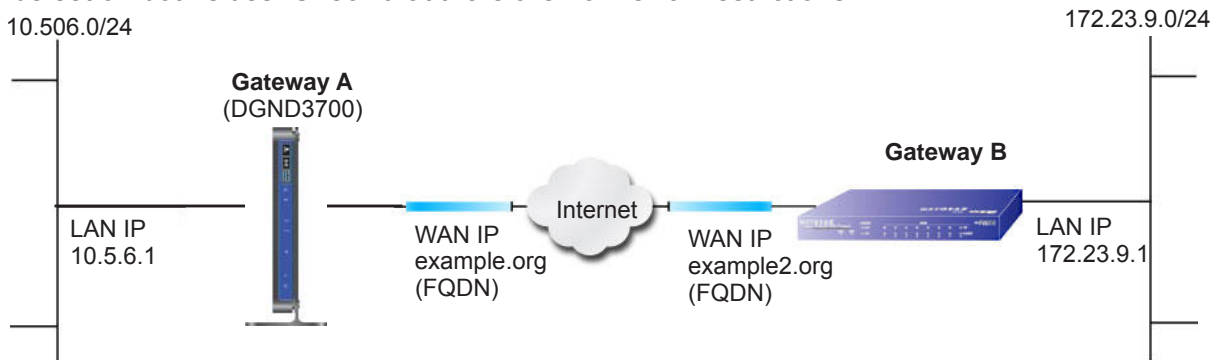
Figure 24. VPNC example, network interface addressing

Table 13. Wireless modem router with FQDN to Gateway B profile summary

VPN Consortium Scenario	Scenario 1
Type of VPN	LAN-to-LAN or gateway-to-gateway (not client-to-gateway)
Security scheme:	IKE with pre-shared secret/key (not certificate based)
IP addressing:	

Table 13. Wireless modem router with FQDN to Gateway B profile summary (Continued)

VPN Consortium Scenario	Scenario 1
Gateway A	Fully qualified domain name (FQDN)
Gateway B	FQDN

Use a Fully Qualified Domain Name (FQDN)

Many ISPs provide connectivity to their customers using dynamic instead of static IP addressing. This means that a user's IP address does not remain constant over time, which presents a challenge for gateways attempting to establish VPN connectivity.

A Dynamic DNS (DDNS) service allows a user whose public IP address is dynamically assigned to be located by a host or domain name. It provides a central public database where information (such as email addresses, host names, and IP addresses) can be stored and retrieved. Now, a gateway can be configured to use a third-party service instead of a permanent and unchanging IP address to establish bidirectional VPN connectivity.

To use DDNS, you have to register with a DDNS service provider. Some DDNS service providers include:

* DynDNS: www.dyndns.org
* TZO.com: netgear.tzo.com
* ngDDNS: ngddns.iego.net

In this example, Gateway A is configured using a sample FQDN provided by a DDNS service provider. In this case the hostname dgnd3800.dyndns.org for Gateway A was provided using the DynDNS service. Gateway B uses the DDNS service provider when establishing a VPN tunnel.

To establish VPN connectivity, Gateway A has to be configured to use Dynamic DNS, and Gateway B has to be configured to use a DNS host name provided by a DDNS service provider to find Gateway A. Again, the following step-by-step procedures assume that you have already registered with a DDNS service provider and have the configuration information necessary to set up the gateways.

Step-by-Step Configuration
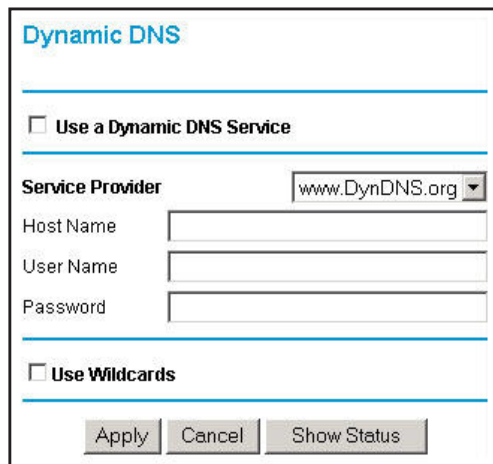
➢ **To configure a VPN tunnel:**

1. Log in to Gateway A (your modem router) as described in *Log In to the N600 Modem Router* on page 18.

   This example assumes that you have set the local LAN address as 10.5.6.1 for Gateway A and have set your own password.

2. On Gateway A, configure the Dynamic DNS settings.

a. Under Advanced, select **Dynamic DNS**.

Dynamic DNS
☐ Use a Dynamic DNS Service
Service Provider   www.DynDNS.org ▼
Host Name   [   ]
User Name   [   ]
Password   [   ]
☐ Use Wildcards
[Apply] [Cancel] [Show Status]

b. Fill in the fields with account and host name settings.

- Select the **Use a Dynamic DNS Service** check box.
- In the **Host Name** field, type **dgnd3800.dyndns.org**.
- In the **User Name** field, enter the account user name.
- In the **Password** field, enter the account password.

c. Click **Apply**.

d. Click **Show Status**. The resulting screen should show Update OK: good:

DDNS Status - Microsoft Internet Explorer

Update OK: good
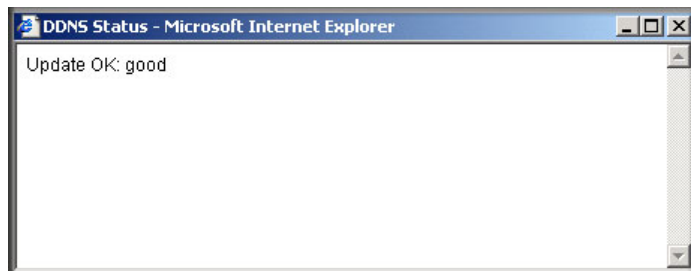
3. On NETGEAR Gateway B, configure the Dynamic DNS settings. Assume a correctly configured DynDNS account.

a. Select **Dynamic DNS**.

b. Select the **DynDNS.org** radio button.

The Dynamic DNS screen displays:

c. Fill in the fields with the account and host name settings.

- In the **Host and Domain Name** field, enter **fvl328.dyndns.org**.

- In the **User Name** field, enter the account user name.

- In the **Password** field, enter the account password.

d. Click **Apply.**

e. Click **Show Status**.

The resulting screen should show Update OK: good:
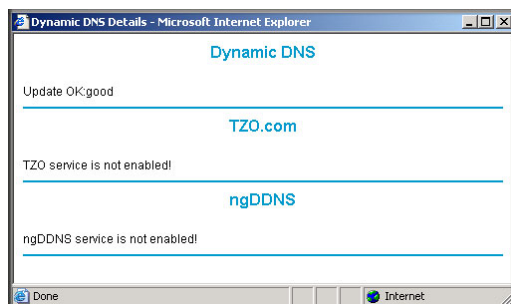
4. Configure the N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B as in the gateway-to-gateway procedures using the VPN Wizard (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 116), being certain to use appropriate network addresses for the environment.

The LAN addresses used in this example are as follows:

Table 14.

Device	LAN IP Address	LAN Subnet Mask
DGND3800B	10.5.6.1	255.255.255.0
FVL328	172.23.6.1	255.255.255.0

    a. For the connection name, enter **toFVL328**.

    b. For the remote WAN's IP address, enter **fvl328.dyndns.org**.

    c. Enter the following:

- IP Address. **172.23.9.1**
- Subnet Mask. **255.255.255.0**

5. Configure the FVL328 as in the gateway-to-gateway procedures for the VPN Wizard (see *Set Up a Gateway-to-Gateway VPN Configuration* on page 116), being certain to use appropriate network addresses for the environment.

    a. For the connection name, enter **toDGND3800**.

    b. For the remote WAN's IP address, enter **dgnd3800.dyndns.org**.

    c. Enter the following:

- IP Address. **10.5.6.1**
- Subnet Mask. **255.255.255.0**

6. Test the VPN tunnel by pinging the remote network from a computer attached to the modem router.

    a. Open the command prompt (select **Start > Run > cmd**)

    b. Type `ping 172.23.9.1`.

```
C:\WINNT\system32\ping.exe

Pinging 172.23.9.1 with 32 bytes of data:

Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
Reply from 172.23.9.1: bytes=32 time<10ms TTL=128
```
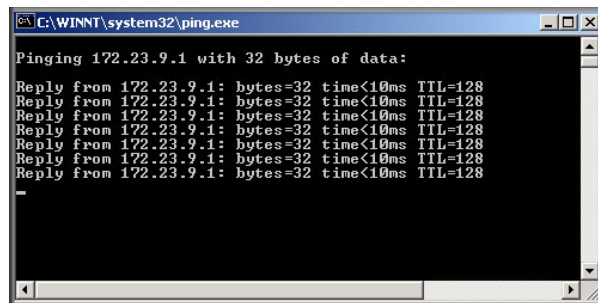
If the pings fail the first time, try the pings a second time.

Configuration Summary (Telecommuter Example)

The configuration in this section follows the addressing and configuration mechanics defined by the VPN Consortium. Gather the necessary information before you begin configuration.

Verify that the firmware is up to date, and make sure you have all the addresses and parameters to be set on both sides. Assure that there are no firewall restrictions.

Table 15. Configuration summary (telecommuter example)

VPN Consortium Scenario	Scenario 1
Type of VPN:	Client-to-gateway, with client behind NAT router
Security scheme:	IKE with pre-shared secret/key (not certificate based)
IP addressing:	
Gateway	Fully qualified domain name (FQDN)
Client	Dynamic
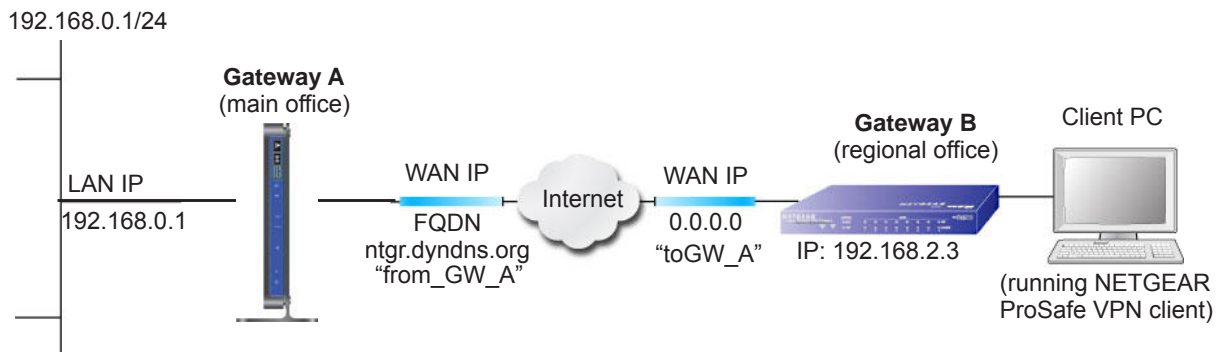
Figure 25. Telecommuter example

Set Up Client-to-Gateway VPN (Telecommuter Example)

Setting up a VPN between a remote computer running the NETGEAR ProSafe VPN client and a network gateway involves two steps, described in the following sections:

- *Step 1: Configure Gateway A (VPN Router at Main Office)* on page 159.
- *Step 2: Configure Gateway B (VPN Router at Regional Office)* on page 160 describes configuring the NETGEAR ProSafe VPN client endpoint.

Step 1: Configure Gateway A (VPN Router at Main Office)

➢ **To configure a VPN tunnel:**

1. Log in to the VPN router. Select **VPN Policies** to display the VPN Policies screen. Click **Add Auto Policy** to proceed and enter the information.

fromGW_A (in the example)

IKE Keep Alive is optional; has to match Remote LAN IP Address when enabled (remote computer has to respond to pings)

192.168.2.3 (in this example) (Remote NAT router has to have Address Reservation set and VPN Passthrough enabled)

fromGW_A.com (in this example)

toGW_A.com (in this example)

2. Click **Apply** when you are finished to display the VPN Policies screen.

To view or modify the tunnel settings, select the radio button next to the tunnel entry, and then click **Edit**.

Step 2: Configure Gateway B (VPN Router at Regional Office)

This procedure assumes that the computer running the client has a dynamically assigned IP address.

The computer has to have a VPN client program installed that supports IPSec (in this case study, the NETGEAR VPN ProSafe Client is used). Go to the NETGEAR website (*www.netgear.com*) for information about how to purchase the NETGEAR ProSafe VPN Client.

Note: Before installing the software, be sure to turn off any virus protection or firewall software you might be running on your computer.

➢ **To configure a VPN tunnel:**

1. Install the NETGEAR ProSafe VPN Client on the remote computer, and then reboot.

   a. You might need to insert your Windows CD to complete the installation.

   b. If you do not have a modem or dial-up adapter installed in your computer, you might see the warning message stating, "The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed." You can disregard this message.

   c. Install the IPSec component. You might have the option to install either the VPN adapter or the IPSec component or both. The VPN adapter is not necessary.

   d. The system should show the ProSafe icon (⬛) in the system tray after you reboot.

   e. Double-click the system tray icon to open the Security Policy Editor.

2. Add a new connection.

   a. Run the NETGEAR ProSafe Security Policy Editor program, and create a VPN connection.

   b. From the Edit menu of the Security Policy Editor, select **Add > Connection**. A New Connection listing appears in the list of policies.

   c. Rename the new connection to match the connection name you entered in the VPN settings of Gateway A. Choose connection names that make sense to the people using and administrating the VPN.
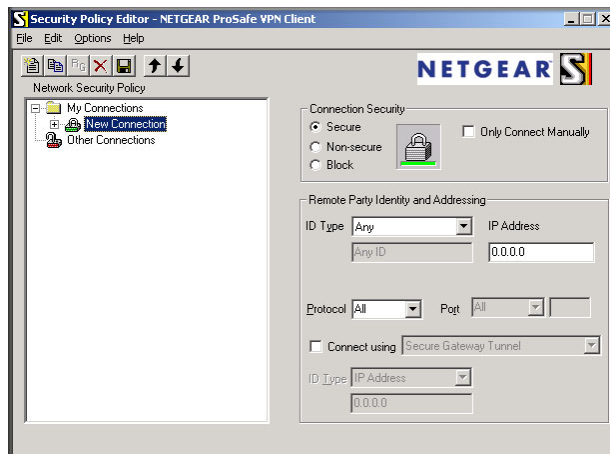
> *Note:* *In this example, the connection name on the client side of the VPN tunnel is toGW_A. It does not have to match the VPN_client connection name used on the gateway side of the VPN tunnel because connection names do not affect how the VPN tunnel functions.*

d. In the Connection Security section, select **Secure**.
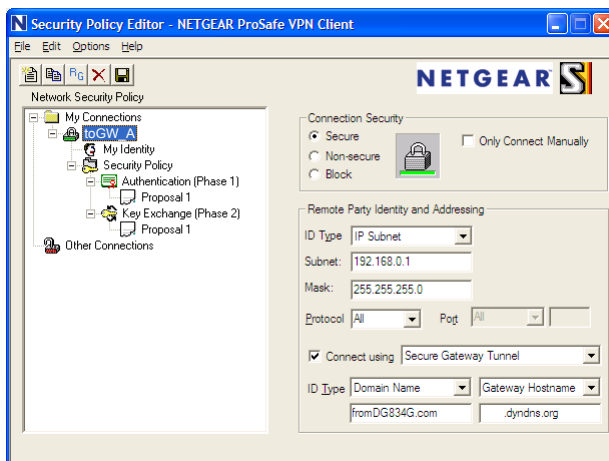
e. In the ID Type drop-down list, select **IP Subnet**.

f. In this example, in the **Subnet** field, type **192.168.0.1** as the network address of the modem router.

g. In the **Mask** field, enter **255.255.255.0** as the LAN subnet mask of the modem router.

h. In the Protocol drop-down list, select **All** to allow all traffic through the VPN tunnel.

i. Select the **Connect using Secure Gateway Tunnel** check box.

j. In the ID Type drop-down list, select **Domain Name**, and enter **fromGW_A.com** (in this example).

k. Select **Gateway Hostname** and enter **ntgr.dyndns.org** (in this example).

3. Configure the security policy in the modem router software.

a. In the Network Security Policy list, expand the new connection by double-clicking its name or clicking the **+** symbol. My Identity and Security Policy appear below the connection name.

b. Click **Security Policy** to show the Security Policy screen.
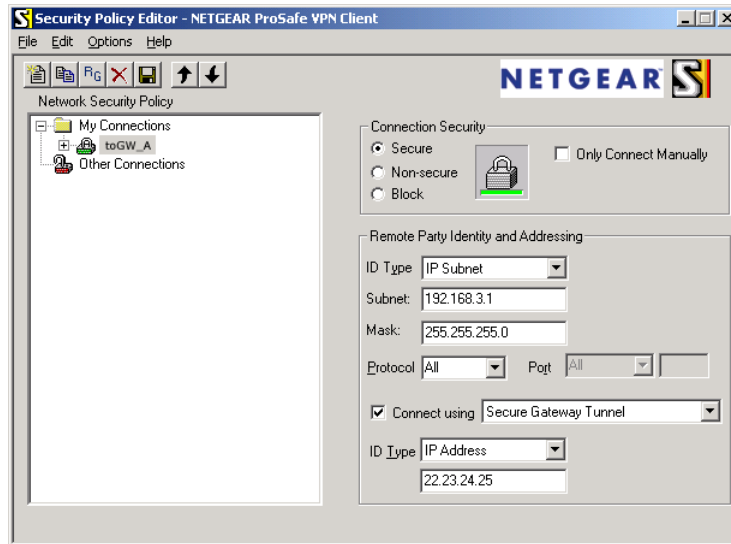
c. In the Select Phase 1 Negotiation Mode group, select the **Main Mode** radio button.

4. Configure the VPN client identity.

In this step, you provide information about the remote VPN client computer. You have to provide the pre-shared key that you configured in the modem router and either a fixed IP address or a fixed virtual IP address of the VPN client computer.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, click **My Identity**.
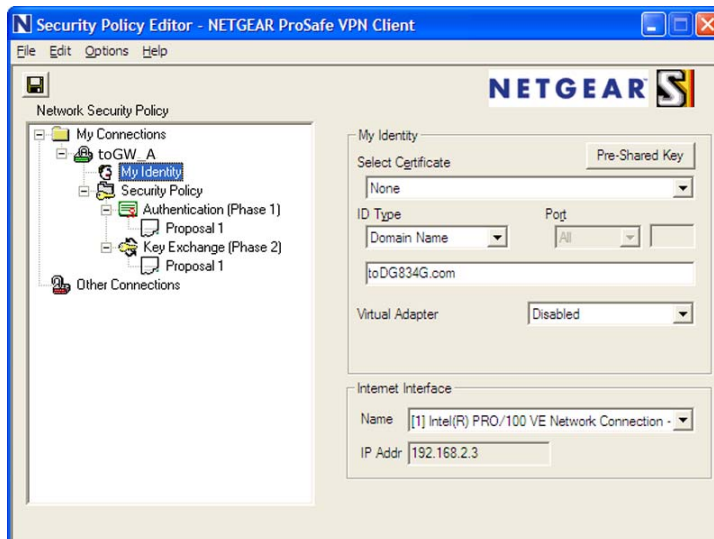
b. In the Select Certificate list, select **None**.

c. In the ID Type list, select **Domain Name**, and enter **toGW_A.com** (in this example).

d. In the Virtual Adapter list, select **Disabled**.

e. In the Internet Interface section, in the Name list, select **Intel PRO/100VE Network Connection** (in this example; your Ethernet adapter might be different), and then in the IP Addr field, enter **192.168.2.3** (in this example).

f. Click the **Pre-Shared Key** button.

g. In the Pre-Shared Key screen, click **Enter Key**. Enter the N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B's pre-shared key and click **OK**. In this example, 12345678 is entered, though the screen shows asterisks. This field is case-sensitive.

5. Configure the VPN Client Authentication Proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the VPN router configuration.

a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double-clicking its name or clicking the + symbol.

b. Expand the Authentication subheading by double-clicking its name or clicking the + symbol. Then select **Proposal 1** below Authentication.

c. In the Authentication Method drop-down list, select **Pre-Shared Key**.

d. In the Encrypt Alg drop-down list, select the type of encryption. In this example, use **Triple DES**.

e. In the Hash Alg drop-down list, select **SHA-1**.

f. In the SA Life drop-down list, select **Unspecified**.

g. In the Key Group drop-down list, select **Diffie-Hellman Group 2**.

6. Configure the VPN Client Key Exchange Proposal.

In this step, you provide the type of encryption (DES or 3DES) to be used for this connection. This selection has to match your selection in the VPN router configuration.

a. Expand the Key Exchange subheading by double-clicking its name or clicking the **+** symbol. Then select **Proposal 1** below Key Exchange.

b. In the SA Life drop-down list, select **Unspecified**.

c. In the Compression drop-down list, select **None**.

d. Select the **Encapsulation Protocol (ESP)** check box.

e. In the Encrypt Alg drop-down list, select the type of encryption. In this example, use **Triple DES**.

f. In the Hash Alg drop-down list, select **SHA-1**.

g. In the Encapsulation drop-down list, select **Tunnel**.

h. Leave the **Authentication Protocol (AH)** check box cleared.

7. Save the VPN client settings.

From the File menu at the top of the Security Policy Editor window, select **Save**.

After you have configured and saved the VPN client information, your computer automatically opens the VPN connection when you attempt to access any IP addresses in the range of the remote VPN router's LAN.

8. Check the VPN connection.

To check the VPN connection, you can initiate a request from the remote computer to the VPN router's network by using the Connect option in the modem router screen:
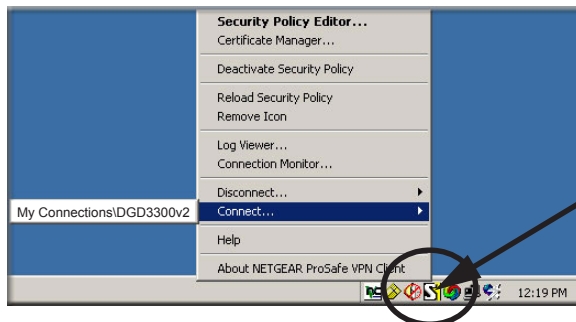
Right-click the system tray icon to open the pop-up menu.

Since the remote computer has a dynamically assigned WAN IP address, it has to initiate the request.

a. Right-click the system tray icon to open the pop-up menu.

b. Select **Connect** to open the My Connections list.

c. Select **toDGND3800**.

The modem router reports the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.

Right-click the system tray icon to open the pop-up menu.

To perform a ping test using this example, start from the remote computer:

a. Establish an Internet connection from the computer.

b. On the Windows taskbar, click the **Start** button, and then select **Run**.

c. Type `ping -t 192.168.0.1`, and then click **OK**.
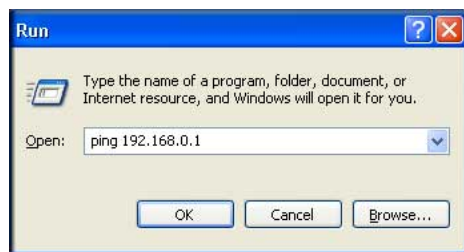
This causes a continuous ping to be sent to the VPN router. Within 2 minutes, the ping response should change from `timed out` to `reply`.

Once the connection is established, you can open the browser on the computer and enter the LAN IP address of the VPN router. After a short wait, you should see the login screen of the VPN router (unless another computer already has the VPN router management interface open).

Note: You can use the VPN router diagnostics to test the VPN connection from the VPN router to the client computer. To do this, log in to the modem router and select **Maintenance > Diagnostics**.

Monitoring the VPN Tunnel (Telecommuter Example)

To view information about the progress and status of the VPN client connection, open the Log Viewer. In Windows, click **Start**, and select **Programs > N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B > Log Viewer**.

Note: Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

The Connection Monitor screen displays:
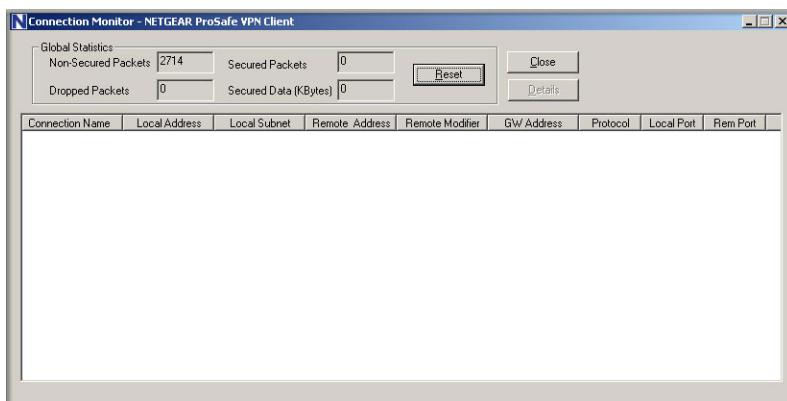
While the connection is being established, the connection name listed in this screen shows SA before the name of the connection. When the connection is successful, the SA changes to the yellow key symbol.

Note: While your computer is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you need to close the VPN connection to have normal Internet access.

View the VPN Router's VPN Status and Log Information

To view information about the status of the VPN client connection, open the VPN router's VPN Status screen:

➢ **To view status and log information:**

1. Select **Maintenance > Router Status**, and then click the **VPN Status** button. The VPN Status/Log screen displays:
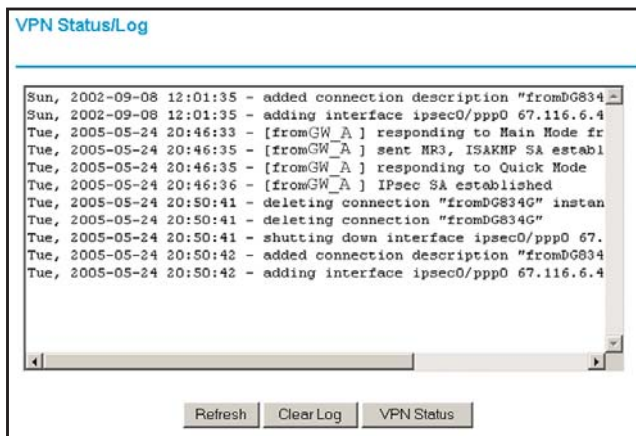
2. To view the VPN tunnels status, click **VPN Status**.
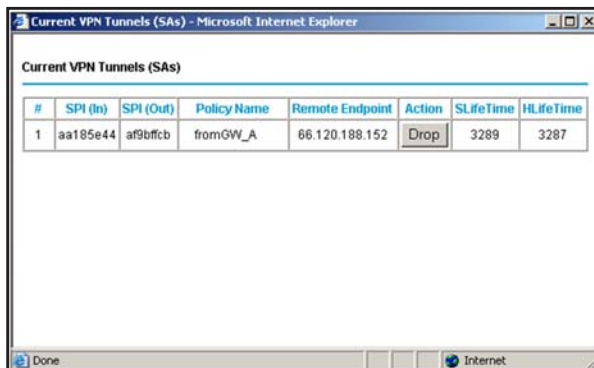
Notification of Compliance

NETGEAR Dual Band - Wireless

C

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe - EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4Ghz), EN301 489-17, EN301 893 (5Ghz), EN60950-1

For complete DoC please visit the NETGEAR EU Declarations of Conformity website at:
http://support.netgear.com/app/answers/detail/a_id/11621/

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Notification of Compliance

Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N600 Wireless Dual Band Gigabit VDSL2 Modem Router DGND3800B complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

* This device may not cause harmful interference, and
* This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

* Reorient or relocate the receiving antenna.
* Increase the separation between the equipment and the receiver.
* Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
* Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

* Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
* This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

The device for the band 5150-5250 MHz is only for indoor usage to reduce po-tential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Avertissement:

Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utili-sation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Index